PCT/JP2004/003945

日本国特許庁
JAPAN PATENT OFFICE

23. 3. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

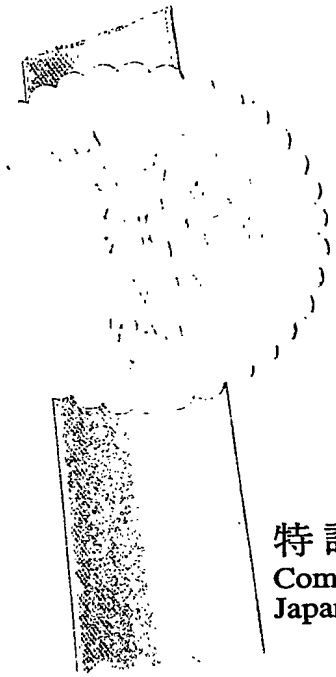
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２４日

出願番号
Application Number: 特願２００３－０８０２６６

[ST. 10/C]: [ＪＰ２００３－０８０２６６]

出願人
Applicant(s): 松下電器産業株式会社



２００４年　４月２２日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０３４３６６

【書類名】　特許願
【整理番号】　2037340001
【提出日】　平成15年 3月24日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　9/06
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　ダニエル　ウェーバー
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　ステファン　ウォルター
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　窪田　憲一
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　データ保護管理装置およびデータ保護管理方法

【特許請求の範囲】

【請求項１】　ライセンスを用いたデータ配信におけるデータ保護管理装置であって、Ｉ／Ｏポートを通してデータとライセンスの通信が行われ、

前記Ｉ／Ｏポートを介して行われる、コンカレントな、セキュアなもしくは通常の、接続を管理し、前記接続の相手との信任状の交換と相互認証を確立し、確立した前記接続での前記ライセンスとそれに続く前記データへのアクセス制限を適用する処理を行うセッションマネージャ部と、

前記セッションマネージャ部で確立したセッションによって前記ライセンスを取得、保存、管理するライセンス管理エンジン部と、

前記ライセンス管理エンジン部が管理する前記ライセンスに関連付けられたユーセッジルールを決定し、前記ライセンスや前記データの処理に前記ユーセッジルールを適用するユーセッジルール適用部と、

前記データの暗号化と復号化や署名に必要な公開鍵または共通鍵の暗号アルゴリズムとハッシュアルゴリズムを実装しており、前記セッションでの暗号化プロトコルの機能を提供する暗号エンジン部と、

メモリへのアクセスを制御し、前記暗号エンジン部での暗号化と復号化に必要な領域を提供するメモリ管理部と、

前記データと前記ライセンスとそれらの接続の状態情報を保存するメモリ部とを備えたことを特徴とするデータ保護管理装置。

【請求項２】　システムに固有の鍵を、前記暗号化と復号化のために少なくとも一つ保持することを特徴とする請求項１記載のデータ保護管理装置。

【請求項３】　データ配信処理に基づく状態の変化に関するログ情報を記憶するログ管理エンジン部をさらに備え、前記ログ管理エンジン部は、前記ログ情報の書き込みおよび読み出しを制御することを特徴とする請求項１記載のデータ保護管理装置。

【請求項４】　ライセンスを用いたデータ配信システムにおいて、送信元から送信されたデータを、情報処理装置を介して送信先へ転送する方法であって、

送信元が、配信対象の前記データに関連付けられた鍵を用いて暗号化されたデータを格納するステップと、

送信元から前記情報処理装置へ、前記暗号化されたデータを転送するステップと、

送信元から前記情報処理装置へ、１つ以上の制御命令を含む命令セットを転送するステップと、

前記情報処理装置と送信先の間で、セキュアなデータ通路を確立するステップと、

送信先から前記情報処理装置へ、１つ以上の制御命令を含む命令セットを転送するステップと、

前記情報処理装置が、命令セットに基づいて、前記暗号化されたデータを、前記鍵を用いて複合化して、前記セキュアなデータ通路を介して送信先に転送するステップとを有するデータ保護管理方法。

【請求項５】　請求項４記載のデータ保護管理方法において、

前記命令セットは、前記セキュアなデータ通路で用いられる暗号化の強度を指定する制御命令を含むことを特徴とするデータ保護管理方法。

【請求項６】　請求項４記載のデータ保護管理方法において、

前記命令セットは、前記セキュアなデータ通路が有効である期間について示す制御命令を含むことを特徴とするデータ保護管理方法。

【請求項７】　請求項４記載のデータ保護管理方法において、

前記命令セットは、前記セキュアなデータ通路を介して、前記データの複製を送信先にいくつ送信するかを示す制御命令を含むことを特徴とするデータ保護管理方法。

【請求項８】　請求項４記載のデータ保護管理方法において、

前記命令セットは、送信元から前記情報処理装置へ転送された制御命令を含むことを特徴とするデータ保護管理方法。

【請求項９】　請求項４記載のデータ保護管理方法において、

前記命令セットは、送信先から前記情報処理装置へ転送された制御命令を含むことを特徴とするデータ保護管理方法。

【請求項１０】　請求項４記載のデータ保護管理方法において、

前記命令セットは、送信先が適合すべき要求事項を示す制御命令を含むことを特徴とするデータ保護管理方法。

【請求項１１】　ライセンスを用いたデータ配信システムにおいて、送信先から送信されたデータを、情報処理装置を介して送信先へ転送する方法であって、

送信元が、配信対象の前記データに関連付けられた鍵を用いて前記データを暗号化するステップと、

送信元から前記情報処理装置へ、前記暗号化されたデータを転送するステップと、

送信元から前記情報処理装置へ、暗号化に用いた前記鍵を転送するステップと、

送信元から前記情報処理装置へ、１つ以上の制御命令を含む命令セットを転送するステップと、

前記情報処理装置が、命令セットに基づいて、前記暗号化されたデータを前記鍵を用いて複合化して、送信先に関連付けられた鍵を用いて前記データを再暗号化するステップとを有するデータ保護管理方法。

【請求項１２】　請求項１１記載のデータ保護管理方法において、

前記命令セットは、再暗号化に許される計算時間について示す制御命令を含むことを特徴とするデータ保護管理方法。

【請求項１３】　請求項１１記載のデータ保護管理方法において、

前記命令セットは、前記データの再暗号化された複製をいくつ生成するかを示す制御命令を含むことを特徴とするデータ保護管理方法。

【請求項１４】　請求項１１記載のデータ保護管理方法において、

前記命令セットは、送信先が適合すべき要求事項を示す制御命令を含むことを特徴とするデータ保護管理方法。

【請求項１５】　請求項１１記載のデータ保護管理方法において、

前記命令セットは、送信先から前記情報処理装置へ転送された制御命令を含むことを特徴とするデータ保護管理方法。

【請求項１６】　ライセンスを用いたデータ配信システムにおいて、送信先か

ら送信されたデータを、情報処理装置を介して送信先へ転送する場合に、前記情報処理装置に格納された所定のライセンスの存在を証明する方法であって、

送信元と前記情報処理装置との間で相互認証を行うステップと、

送信元と前記情報処理装置の間で、セキュアなデータ通路を確立するステップと、

送信元から前記情報処理装置へ、前記所定のライセンスの存在証明を要求するチャレンジを転送するステップと、

前記情報処理装置が、命令セットに基づいて、前記チャレンジと前記所定のライセンスを用いて、固有の証明を生成するステップと、

前記情報処理装置が、前記生成した証明を送信元に転送するステップと、

送信元が、受け取った前記証明を検証するステップとを有するデータ保護管理方法。

【請求項１７】　請求項１６記載のデータ保護管理方法において、

前記証明を生成する際に、前記情報処理装置が、前記チャレンジと前記証明を、送信元の公開鍵を用いて暗号化することを特徴するデータ保護管理方法。

【請求項１８】　請求項１６記載のデータ保護管理方法において、

前記証明を生成する際に、前記情報処理装置が、前記生成した証明を前記ライセンスに含まれる鍵を用いて暗号化することを特徴とするデータ保護管理方法。

【請求項１９】　請求項１６記載のデータ保護管理方法において、

前記生成した証明を送信元に転送する際に、前記ライセンスに含まれる付加的なデータとともに前記証明を送信元に転送することを特徴とするデータ保護管理方法。

【請求項２０】　請求項１９記載のデータ保護管理方法において、

前記付加的なデータを前記ライセンスに含まれる鍵を用いて暗号化することを特徴とするデータ保護管理方法。

【請求項２１】　請求項１９記載のデータ保護管理方法において、

前記命令セットは、前記ライセンスに基づいて、前記証明に付加されるデータを決定する情報を含むことを特徴とするデータ保護管理方法。

【請求項２２】　ライセンスを用いたデータ配信システムにおいて、送信先か

ら送信されたデータを、情報処理装置を介して送信先へ転送する場合に、前記情報処理装置に格納された所定のライセンスの状態情報を変更する方法であって、

送信元と前記情報処理装置との間で相互認証を行うステップと、

送信元と前記情報処理装置の間で、セキュアなデータ通路を確立するステップと、

送信先から前記情報処理装置へ、前記所定のライセンスの状態情報の変更を要求するとともに、ライセンスの存在証明を要求するチャレンジを転送するステップと、

前記情報処理装置が、前記要求に従い、前記所定のライセンスの状態情報を変更するステップと、

前記情報処理装置が、命令セットに基づいて、前記チャレンジと前記所定のライセンスを用いて、固有の証明を生成するステップと、

前記情報処理装置が、前記生成した証明を送信元に転送するステップと、

送信元が、受け取った前記証明を検証するステップとを有するデータ保護管理方法。

【請求項２３】　ライセンスを用いたデータ配信システムにおいて、送信先から送信されたデータを、情報処理装置を介して送信先へ転送する場合に、前記情報処理装置に所定のライセンスを格納する方法であって、

送信元と前記情報処理装置との間で相互認証を行うステップと、

送信元と前記情報処理装置の間で、セキュアなデータ通路を確立するステップと、

送信元から前記情報処理装置へ、前記所定のライセンスを転送するステップと、

前記情報処理装置は、命令セットに基づき、前記受け取った所定のライセンスを格納するステップとを有するデータ保護管理方法。

【請求項２４】　ライセンスを用いたデータ配信システムにおいて、送信先から送信されたデータを、情報処理装置を介して送信先へ転送する場合に、前記情報処理装置に所定のライセンスを格納する方法であって、

送信元と前記情報処理装置との間で相互認証を行うステップと、

前記情報処理装置から送信元へ、送信先に関連付けられた公開鍵を転送するステップと、

送信元が、前記受け取った公開鍵を用いて、前記所定のライセンスを暗号化し、前記暗号化したライセンスを前記情報処理装置へ転送するステップと、

前記情報処理装置が、送信先に関連付けられた秘密鍵を用いて、前記暗号化したライセンスを複合化するステップとを有するデータ保護管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルデータを保護する装置および方法に関し、特に、ライセンスを用いたデータ配信における配信データおよびライセンスデータ、及び電子チケットの保護に関する。

【０００２】

【従来の技術】

近年、ユーザが、コンテンツプロバイダーが作成したデジタルコンテンツをネットワーク経由で取得して再生する、データ配信サービスが普及してきた。サービスを提供するコンテンツプロバイダーは、彼らが所有する知的財産が著作権侵害を受けたり、不正に複製・乱用されたりすることがないと判断した場合に、デジタルコンテンツの使用を認めている。

【０００３】

デジタルコンテンツのセキュリティを提供する技術として、ユーザの識別子を用いたユーザ毎に専用の秘密アルゴリズムを用いることにより、デジタルコンテンツの不正使用を防御する方法があった（例えば、特許文献１参照）。これにより、専用の再生機器、或いは対応可能なＰＣハードウェアで固有なＩＤ（デバイス依存）を持つものでしかデジタルコンテンツを再生できないように制限することが可能となり、不正な複製からデータを保護することができる。

【０００４】

図１８は、従来のデータ配信システムの概要を示す図である。このシステムは、サーバであるコンテンツプロバイダー１００（以下、サーバと記載する）と、

ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）１０４と、クライアント１０６とを備えている。サーバ１００とＰＣ１０４は、ネットワークを介して接続可能であり、クライアント１０６は、サーバ１００からネットワーク経由で配信されたコンテンツに対し、記憶保持や再生などの処理を行う装置である。サーバ１００内のコンテンツ記憶装置１０２よりコンテンツを取得する際、サーバ１００は、クライアント１０６より通知されたシリアルナンバー（または、デバイスナンバー）を暗号化の鍵１０１とし、この暗号化の鍵１０１を用いて配信対象のコンテンツを暗号化する（１０３）。このシリアルナンバー自体を暗号化の鍵として使用するだけでなく、暗号化に必要な鍵やパスワードを生成するために用いられてもよい。暗号化されたコンテンツは、ＰＣ１０４を介してクライアント１０６に転送される。なお、ＰＣ１０４は、暗号化されたコンテンツを受信した際に、即時にクライアント１０６に通知するのでなく、任意のタイミングでクライアント１０６に通知してもよい。また、ＰＣ１０４上にアーガイブとしてまとめて管理してもよい。このため、ＰＣ１０４内の暗号化コンテンツ記憶装置１０５に、配信された暗号化されたコンテンツを記憶してもよい。クライアント１０６は、受信した暗号化されたコンテンツを、組み込まれた復号化の鍵１０９を用いて復号化処理を行い（１０７）、復号化されたコンテンツをコンテンツ記憶装置１０８に格納する。また、コンテンツ記憶装置１０８に格納せずに、オンザフライの再生を行う。

【０００５】

以上のように、クライアントからサーバにシリアルナンバーを通知し、サーバが受信したシリアルナンバーに基づいて暗号化したコンテンツデータをクライアントに送信することにより、コンテンツデータの配信を行う。

【０００６】

図１９も、従来のデータ配信システムの概要を示す図である。このシステムは、サーバであるコンテンツプロバイダー２０１（以下、サーバと記載する）と、ＰＣ２０５と、クライアント２１１とを備えている。サーバ２０１内のコンテンツ記憶装置２０２に格納されているコンテンツを配信する際、サーバ２０１は、コンテンツかユーザかクライアント２１１に関連つけられた鍵を生成し（２０３

）、この鍵を用いてコンテンツの暗号化を行う（２０４）。ＰＣ２０５は、サーバ２０１にコンテンツの取得要求を通知することにより、暗号化されたコンテンツと、これに関連付けられた鍵をサーバ２０１から受け取り、それぞれコンテンツ記憶装置２０６と、鍵記憶装置２０７に格納する。ＰＣ２０５は、コンテンツ記憶装置２０６に格納されたコンテンツをクライアント２１１へ通知する前に、鍵記憶装置２０７に格納されている関連つけられた鍵を用いてコンテンツの復号化を行い（２０８）、クライアント２１１から、もしくは、クライアント２１１への通知のセッションから得られた鍵２１０を用いて、コンテンツを再び暗号化する（２０９）。クライアント２１１は、受信した暗号化されたコンテンツをコンテンツ記憶装置２１２に格納する。この場合、コンテンツを再生するなどメディア出力する前に、セッション鍵記憶装置２１４に格納されているセッション鍵を用いて、復号化を行う（２１５）。なお、受信した暗号化されたコンテンツを、まず復号化を行い、コンテンツ記憶装置２１２に格納してもよい。

【０００７】

以上のように、サーバが生成した鍵とその鍵を用いて暗号化したコンテンツデータをＰＣに通知し、ＰＣとクライアント間で別の鍵（セッション鍵）を用いて再暗号化することにより、コンテンツデータの配信を行う。

【０００８】

【特許文献１】

特開平７－２９５８００号公報

【０００９】

【発明が解決しようとする課題】

しかしながら、上述した従来の技術では、不正な複製からデータを保護するために、専用の再生機器や、対応可能なＰＣハードウェアで固有なＩＤ（デバイス依存）を持つものでしか取得したコンテンツデータの再生ができない。そのため、ユーザがＯＳやハードウェアのアップデートを行うことにより、今まで再生できていたコンテンツデータの再生ができなくなる可能性がある。また、再生に専用の再生機器が必要になるのでは、ユーザが利用したい時に、いつでも、どこでもコンテンツデータを楽しむことが難しい。

【００１０】

また、専用の再生機器でしか再生することができないため、メモリカードやＩＣカード、ＳＤカード、ＣＤ－Ｒなどの着脱可能な記録媒体にコンテンツデータを格納した場合でも、他の再生専用装置を用いて再生処理することができない。

【００１１】

また、現在のシステムでは、ＰＣとネットワークへの接続環境がないユーザは、コンテンツプロバイダーが用意したコンテンツを利用することができない。

【００１２】

本発明は、上記問題点を解決するためになされたものであり、デジタルデータの乱用や不正利用を防止し、且つユーザに再生機器に対する選択の自由を与え、デジタルデータを利用する際の保護機能を強化することを目的としている。また、コンテンツ配信手段としてネットワークのみに依存せず、その他の配信チャネルによるデータ配信も利用可能とすることを目的としている。

【００１３】

【課題を解決するための手段】

上記課題を解決するために、本発明のデータ保護装置は、接続を管理し、前記接続の相手との信任状の交換と相互認証を確立し、確立した前記接続でのライセンスとそれに続く前記データへのアクセス制限を適用する処理を行うセッションマネージャ部と、前記セッションマネージャ部で確立したセッションによって前記ライセンスを取得、保存、管理するライセンス管理エンジン部と、前記ライセンス管理エンジン部が管理する前記ライセンスに関連付けられたユーセッジルールを決定し、前記ライセンスや前記データの処理に前記ユーセッジルールを適用するユーセッジルール適用部と、前記データの暗号化と復号化や署名に必要な公開鍵または共通鍵の暗号アルゴリズムとハッシュアルゴリズムを実装しており、前記セッションでの暗号化プロトコルの機能を提供する暗号エンジン部と、メモリへのアクセスを制御し、前記暗号エンジン部での暗号化と復号化に必要な領域を提供するメモリ管理部と、前記データと前記ライセンスとそれらの接続の状態情報を保存するメモリ部とを備えることを特徴とする、以下、このデータ保護管理装置をセキュアコンテナと記載する。

【００１４】

これにより、デジタルライセンスデータをセキュアに保存・送信するための暗号化アルゴリズムやプロトコルを提供することによって、ライセンスデータの安全管理を保証できる。

【００１５】

また、本発明のデータ保護管理装置は、システムに固有の鍵を暗号化と復号化のために少なくとも一つ保持することを特徴とする。これにより、システムに固有な鍵をコンテンツの暗号化に用いることが可能となり、データの盗聴や改ざんを防ぐ安全性をより強化できる。

【００１６】

また、本発明のデータ保護管理装置は、データ配信処理に基づく状態の変化に関する情報を記憶するログ管理エンジン部を更に備え、ログ情報の書き込みおよび読み出しを制御することを特徴とする。これにより、セキュアコンテナがトランザクションの記録やその他のセキュリティに関する操作を行うことが可能となり、セキュアコンテナやそこに保存されているデジタルライセンスデータが改ざんや乱用を受けた場合、システム制作者や許可された第三者がそれを認識できるようになる。

【００１７】

また、本発明のデータ保護管理方法は、送信元が、配信対象のデータに関連付けられた鍵を用いて暗号化されたデータを格納するステップと、送信元から情報処理装置へ、前記暗号化されたデータを転送するステップと、送信元から前記情報処理装置へ、１つ以上の制御命令を含む命令セットを転送するステップと、前記情報処理装置と送信先の間で、セキュアなデータ通路を確立するステップと、送信先から前記情報処理装置へ、１つ以上の制御命令を含む命令セットを転送するステップと、前記情報処理装置が、命令セットに基づいて、前記暗号化されたデータを、前記鍵を用いて複合化して、前記セキュアなデータ通路を介して送信先に転送するステップとを有することを特徴とする。この命令セットは、ユーセッジルールとも呼ばれる。また、送信元をソース、送信先をシンクとも呼ぶ。さらに、この情報処理装置は、前述したセキュアコンテナを示す。これにより、セ

キュアコンテナを通してデータを転送するので、要求される操作や制御を適用しながら安全にデータをソースからシンクに送付できる。

【００１８】

また、本発明のデータ保護管理方法は命令セットとして、セキュアなデータ通路で用いられる暗号化の強度を指定する制御命令を含むことを特徴とする。これにより、制御命令で暗号化の強度（つまり、セキュアコンテナとシンク間のセキュアなチャネルの強度）を管理することで、データ通路の種類に応じてより柔軟に安全性を向上することができる。

【００１９】

また、本発明のデータ保護管理方法は、命令セットとして、セキュアなデータ通路が有効である期間について示す制御命令を含むことを特徴とする。これにより、暗号化（セキュアコンテナとシンク間のセキュアなチャネル）を管理する制御命令は、再暗号化が可能な期間を定義可能となり、顧客が、購買期間中に（放送データなどを）個人用にコピー保存したり、データを計画利用できたりする購買型システムを確立することができる。

【００２０】

また、本発明のデータ保護管理方法は、命令セットとして、データの複製をシンクにいくつ送信するかを示す制御命令を含むことを特徴とする。これにより、暗号化（セキュアコンテナとシンク間のセキュアなチャネル）を管理する制御命令は、セキュアコンテナに送信可能なコピー回数を規定することにより、データのバックアップや共有に有用である。コンテンツは顧客に対応付けられているので、監視や監査が可能である。

【００２１】

また、本発明のデータ保護管理方法は、命令セットとして、送信元から情報処理装置へ転送された制御命令を含むことを特徴とする。これにより、ソースからセキュアコンテナに送られる制御命令セットを追加することが可能となり、ソースがセキュリティ要件を規定できるなどの利点がある。ライセンスや鍵に付随する制御セットに定義されているデフォルト要件が弱められることはない。

【００２２】

また、本発明のデータ保護管理方法は、命令セットとして、送信先から情報処理装置へ転送された制御命令を含むことを特徴とする。これにより、シンクからセキュアコンテナに送られる制御命令セットを追加することが可能となり、シンクがセキュリティ要件を規定できるなどの利点がある。ライセンスや鍵に付随する制御セットに定義されているデフォルト要件が弱められることはない。

【００２３】

また、本発明のデータ保護管理方法は、命令セットとして、送信先が適合すべき要求事項を示す制御命令を含むことを特徴とする。これにより、暗号化（セキュアコンテナとシンク間のセキュアなチャネル）を管理する制御命令は、シンクに対する要件を定義することが可能となり、ソースがシンクに要件を指示することができる。例えば、シンクは購入するのに高額なデータに対してはユーザによる確認といった一定のセキュリティ基準に従わなければならないなどの要件を定義できる。

【００２４】

また、本発明のデータ保護管理方法は、送信元が、配信対象のデータに関連付けられた鍵を用いて前記データを暗号化するステップと、送信元から前記情報処理装置へ、前記暗号化されたデータを転送するステップと、送信元から前記情報処理装置へ、暗号化に用いた前記鍵を転送するステップと、送信元から前記情報処理装置へ、１つ以上の制御命令を含む命令セットを転送するステップと、前記情報処理装置が、命令セットに基づいて、前記暗号化されたデータを前記鍵を用いて複合化して、送信先に関連付けられた鍵を用いて前記データを再暗号化するステップとを有することを特徴とする。これにより、再暗号化処理では、シンクに対応付けられたデータの個別化を行うことが可能となり、暗号化が行われると、データを復号できるのは対応するシンクのみとなり、より安全性を高めることができる。

【００２５】

また、本発明のデータ保護管理方法は、命令セットとして、再暗号化に許される計算時間について示す制御命令を含むことを特徴とする。これにより、顧客が購買期間中に（放送データなどを）個人用にコピー保存することが可能な購買シ

ステムが確立できる。

【００２６】

また、本発明のデータ保護管理方法は、命令セットとして、データの再暗号化された複製をいくつ生成するかを示す制御命令を含むことを特徴とする。これにより、再暗号化を管理する制御命令は、コピー可能回数を規定する。データのバックアップや共有に有用で、コンテンツが顧客に対応付けられているので、監視や監査が可能である。

【００２７】

また、本発明のデータ保護管理方法は、命令セットとして、送信先が適合すべき要求事項を示す制御命令を含むことを特徴とする。これにより、再暗号化を管理する制御命令は、シンクに対する要件を規定することが可能となり、ソースはシンクに要件を指示することができる。例えば、シンクは購入するのに高額なデータに対しては一定のセキュリティ基準に従わなければならないなどの要件を指定できる。

【００２８】

また、本発明のデータ保護管理方法は、命令セットとして、送信先から前記情報処理装置へ転送された制御命令を含むことを特徴とする。これにより、再暗号化プロセスを管理する制御命令がシンクに存在することが可能であり、シンクが独立して再暗号化を行うことができるという利点がある。また、制御命令はソースに存在し、暗号化はソースで行われることにより、データ製作者や所有者に対応しているソースが、再暗号化プロセスを完全に制御できるという利点がある。本発明では、顧客がコンテンツを個別化するこができるので、他人にコンテンツを利用されることがない。コンテンツは再暗号化プロセスで匿名化することもできる。

【００２９】

また、本発明のデータ保護管理方法は、情報処理装置に格納された所定のライセンスの存在を証明する方法であって、送信元と前記情報処理装置との間で相互認証を行うステップと、送信元と前記情報処理装置の間で、セキュアなデータ通路を確立するステップと、送信元から前記情報処理装置へ、前記所定のライセン

スの存在証明を要求するチャレンジを転送するステップと、前記情報処理装置が、命令セットに基づいて、前記チャレンジと前記所定のライセンスを用いて、固有の証明を生成するステップと、前記情報処理装置が、前記生成した証明を送信元に転送するステップと、送信元が、受け取った前記証明を検証するステップとを有することを特徴とする。これにより、ソースにそのライセンスの詳細情報を与えずに、シンクにライセンスが存在することを証明することが可能となる。つまり、シンクのライセンスプールにライセンスが存在すること示す証明を受け取りたい場合、ソースはセキュアなチャネルを利用してシンクに証明書の発行請求を出さなければならない。シンク（セキュアコンテナ）は、ソースからシンクに送られた要求（チャレンジ）を考慮に入れて証明書を生成する。生成された証明書は、セキュアなチャネルを通してソースに送られる。ライセンスに固有な証明書を発行する利点は、シンクがライセンスの詳細情報をソースに送る必要がない点である。また、この証明書は、ライセンスが電子チケットの代わりになる電子チケットシステムでも利用可能である。さらに、ソースから受け取った命令セットを用いることにより、ライセンス発行者が証明書の生成方法を制御できる。

【００３０】

また、本発明のデータ保護管理方法は、証明を生成する際に、情報処理装置が、チャレンジと証明を、送信元の公開鍵を用いて暗号化することを特徴する。これにより、公開鍵方式を利用して証明を暗号化することが可能となり、ソースとセキュアコンテナ間の接続をセキュアにする必要性がないという利点がある。この場合、セキュリティは公開鍵方式で実現される。ここで、ソースの公開鍵は、ライセンスの一部として組み込まれる可能性がある。

【００３１】

また、本発明のデータ保護管理方法は、証明を生成する際に、情報処理装置が、生成した証明をライセンスに含まれる鍵を用いて暗号化することを特徴とする。これにより、ライセンスの一部を鍵として利用することが可能となり、ライセンス発行者や許可された第三者のみが証明を復号できる。また、ソースが証明書を復号できるのであれば、そのソースは許可されたものであると考えられることから、ソースが自身の認証をセキュアコンテナに対し行う必要がなくなる。

【００３２】

また、本発明のデータ保護管理方法は、生成した証明を送信元に転送する際に、ライセンスに含まれる付加的なデータとともに証明を送信元に転送することを特徴とする。これにより、ライセンスからの追加データを証明に付け加えた後、証明をソースに転送することが可能となり、この方法で電子チケットを実現することができる。

【００３３】

また、本発明のデータ保護管理方法は、付加的なデータをライセンスに含まれる鍵を用いて暗号化することを特徴とする。これにより、ライセンスからの追加データを証明に添付し、証明と付加データの一方、或いは両方を暗号化し、ソースに転送することが可能となり、この方法で電子チケットを実現することができる。

【００３４】

また、本発明のデータ保護管理方法は、命令セットとして、ライセンスに基づいて、証明に付加されるデータを決定する情報を含むことを特徴とする。これにより、証明生成を管理する制御命令に、ライセンスのどのデータを証明に添付すべきかを示す情報を含めることが可能となり、ライセンスに付随するデータの特定のサブセットを証明に添付することができる。

【００３５】

また、本発明のデータ保護管理方法は、情報処理装置に格納された所定のライセンスの状態情報を変更する方法であって、送信元と前記情報処理装置との間で相互認証を行うステップと、送信元と前記情報処理装置の間で、セキュアなデータ通路を確立するステップと、送信先から前記情報処理装置へ、前記所定のライセンスの状態情報の変更を要求するとともに、ライセンスの存在証明を要求するチャレンジを転送するステップと、前記情報処理装置が、前記要求に従い、前記所定のライセンスの状態情報を変更するステップと、前記情報処理装置が、命令セットに基づいて、前記チャレンジと前記所定のライセンスを用いて、固有の証明を生成するステップと、前記情報処理装置が、前記生成した証明を送信元に転送するステップと、送信元が、受け取った前記証明を検証するステップとを有す

ることを特徴とする。これにより、ライセンスの状態情報は、必要であれば、ライセンスに割り当てられるか、ライセンスの中に組み込まれる。つまり、状態情報を変更したい場合、まずソースとセキュアコンテナ間の相互認証を行い、認証が成功するとセキュアなチャネルが確立される。次に、ライセンス状態情報の変更を要請するリクエストが、ソースからセキュアコンテナに送付され、セキュアコンテナで要求に沿った操作がおこなわれる。ライセンス状態情報の変更が成功すれば、セキュアコンテナは証明をソースに送る。ソースでは、送付された証明から要求した変更の結果を確認できる。この方法の利点は、ライセンス状態情報の変更で、双方向、或いは複数の電子チケットを実現できる点とライセンスに対応するデジタルデータの使用を制限できる点である。

【００３６】

また、本発明のデータ保護管理方法は、情報処理装置に所定のライセンスを格納する方法であって、送信元と前記情報処理装置との間で相互認証を行うステップと、送信元と前記情報処理装置の間で、セキュアなデータ通路を確立するステップと、送信元から前記情報処理装置へ、前記所定のライセンスを転送するステップと、前記情報処理装置は、命令セットに基づき、前記受け取った所定のライセンスを格納するステップとを有することを特徴とする。つまり、セキュアコンテナとソースは相互認証を行い、認証が成功すれば、両者間にセキュアなチャネルが確立される。受理したライセンスデータはセキュアコンテナ内の内部メモリで保存される。これにより、ライセンスをセキュアコンテナに保存する時に、前記ライセンスデータはソースからデバイスへセキュアに転送され、デバイスのメモリに安全に保存される。ライセンスデータは決して平文で公開されることはない。

【００３７】

また、本発明のデータ保護管理方法は、情報処理装置に所定のライセンスを格納する方法であって、送信元と前記情報処理装置との間で相互認証を行うステップと、前記情報処理装置から送信元へ、送信先に関連付けられた公開鍵を転送するステップと、送信元が、前記受け取った公開鍵を用いて、前記所定のライセンスを暗号化し、前記暗号化したライセンスを前記情報処理装置へ転送するステッ

プと、前記情報処理装置が、送信先に関連付けられた秘密鍵を用いて、前記暗号化したライセンスを複合化するステップとを有することを特徴とする。つまり、セキュアコンテナとソースは相互認証を行い、認証が成功すると、デバイスに対応した公開鍵がソースに送付される。ソースでは、受け取った公開鍵を使ってライセンスデータを暗号化し、暗号データをセキュアコンテナに送る。セキュアコンテナでは、受け取ったデータを内部メモリに保存する。これにより、ライセンスをセキュアコンテナに保存する時に、前記ライセンスデータはソースからデバイスへセキュアに転送され、デバイスのメモリに安全に保存される。ライセンスデータは決して平文で公開されることはない。

【００３８】

【発明の実施の形態】

以下、本発明の実施の形態を図面を用いて詳細に説明する。

【００３９】

（実施の形態１）

コンテンツプロバイダーなどのサーバが保持するコンテンツデータを、ネットワークを介して取得するデータ配信システムおいて、コンテンツデータの不正な利用を制限し、データを保護することが求められている。本発明の実施の形態１におけるデータ保護管理装置は、例えば、改竄防止機能付きハードウェアのＩＣカードといった、セキュアなコンテナ内に組み込まれたＤＲＭ（Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ）装置であって、正常なデジタルライセンス管理や、デジタルライセンスやライセンスに関連付けられたデジタルデータ格納制御などを行う。なお、これらは、ハードウェア、ソフトウェアのいずれで実現してもよい。

【００４０】

ライセンスは、関連のあるユーセッジルールを含むものが多い。ユーセッジルールは、前記ライセンスと、前記ライセンスに関連付けられたデジタルデータの利用に関するルールを定義するものである。ユーセッジルールで特定の処理に関するルールが定義されていない場合、予め既定されているデフォルトの設定を適用する。もしデフォルトとユーセッジルールが異なった場合、より制約が強く、

よりセキュアなルールが適用されなければいけない。

【００４１】

図１７は、データ配信システムのネットワーク環境の概要を示したものである。本発明の実施の形態１におけるＤＲＭ装置は、コンテンツプロバイダーやコンテンツサーバからネットワークを介してデジタルデータを取得するクライアントデバイス上に実装される。なお、このネットワークは、有線であっても無線であってもよく、また、インターネットやイントラネット、サーバと１対１で直接接続、インターネットとローカルＬＡＮとの双方と接続するなど、接続形態は限定されない。

【００４２】

次に、本発明の実施の形態１におけるＤＲＭ装置について、詳細を説明する。

【００４３】

ＤＲＭ装置は、ライセンスデータをセキュアに保存・送信するための暗号化アルゴリズムやプロトコルを提供することにより、ライセンスデータの安全管理を保証するものである。なお、データの送信元（ソース）と送信先（シンク）間の追加的なデータセキュリティ層となるカードを通して転送されるデジタルデータにも適用可能である。

【００４４】

以下、ＤＲＭ装置を備え、ライセンスやデジタルデータをセキュアに管理する装置を、セキュアコンテナと呼ぶ。このセキュアコンテナは、耐タンパ性を持ってセキュアなものである。また、ソースから取得したライセンスデータ（またはコンテンツデータ）は、セキュアコンテナ内のメモリに保存される。

【００４５】

ソースとは、コンテンツのデータの提供元であり、コンテンツプロバイダーや、コンテンツサーバなどを指す。

【００４６】

シンクとは、前述したソースからコンテンツデータを取得する送信先であり、クライアントデバイスや再生装置などを指す。例えば、メモリカードやＩＣカード、ＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）カード、ＣＤ－Ｒなどの記録媒体を

備え、これら記録媒体へのＲｅａｄ／Ｗｒｉｔｅ機能を有する装置である。なお、コンテンツデータの再生は、記録媒体を着脱することにより、他の再生専用装置を用いて実行することが可能である。

【００４７】

図１は、本発明の実施の形態１におけるセキュアコンテナの構成を示す機能ブロック図である。

【００４８】

セキュアコンテナ５００は、Ｉ／Ｏポート５０１と、セッションマネージャ５０２と、ライセンス管理エンジン５０６と、ユーセッジルール適用部５０５（ユーセッジルールは、命令セットとも呼ぶ）と、暗号エンジン５０７と、メモリ管理部５０３と、メモリ５０４とを備えている。

【００４９】

セッションマネージャ５０２は、Ｉ／Ｏポート５０１を介して行われる接続を管理する。ここでの接続とは、通常の接続だけでなく、暗号化エンジン５０７を用いたセキュアな通信を行うことも可能である。セッションマネージャ５０２は、接続相手と信任状の交換と相互認証することでセッションを確立し、確立したセッションにおける、ライセンスデータとそれに続くコンテンツデータへのアクセス許可などのアクセス制限管理を可能とする。

【００５０】

ライセンス管理エンジン５０６は、セッションマネージャ５０２で確立したセッションにおいて、Ｉ／Ｏポート５０１を介してライセンスデータを取得し、取得したライセンスデータの保存、及び管理を行う。

【００５１】

ユーセッジルール適用部５０５は、ライセンス管理エンジン５０６が管理する処理対象のライセンスデータに関連付けられたユーセッジルールを決定し、ライセンスデータやコンテンツデータの処理に、この決定したユーセッジルールを適用する。

【００５２】

暗号エンジン５０７は、コンテンツデータの暗号化と復号化や署名に必要な公

開鍵または共通鍵の暗号アルゴリズムとハッシュアルゴリズムを保持しており、セッションマネージャ５０２が確立したセッションでの暗号化プロトコルの機能を提供する。

【００５３】

メモリ管理部５０３は、メモリ５０４へのアクセスを制御し、暗号エンジン５０７での暗号化と復号化に必要な領域を提供する。メモリ５０４は、コンテンツデータとライセンスデータと、接続の状態情報を、記憶保持する。

【００５４】

以上により、セキュアコンテナは、デジタルライセンスデータをセキュアに保存・送信するための暗号化アルゴリズムやプロトコルを提供することが可能となり、ライセンスデータの安全管理を保証することができる。

【００５５】

また、デジタルライセンスが普通のテキスト形式でもセキュアコンテナの外に出ることが決してないこと、必要な操作はすべてセキュアコンテナ内で行われることである。

【００５６】

なお、このセキュアコンテナを、その全て或いは一部をソフトウェアで実装することにより、携帯電話などの機器にセキュアコンテナを実装することができる。更に、このセキュアコンテナを、メモリカード型のストレージデバイスに埋め込むことにより、ＳＤカードなどのメモリカード型デバイスにセキュアコンテナを実装することにより、基本的に、デジタルライセンスやデータ管理用メモリカード型デバイスの製造が可能になる。または、従来のデータ記憶装置に新たに機能が加わったデジタルライセンス及びデータ管理用メモリカード型デバイスの製造が可能になる。

【００５７】

また、本発明の実施の形態１におけるセキュアコンテナのメモリに、ＩＳＯ／ＩＥＣ９２９３に準拠したＦＡＴファイルシステムを組み込むことにより、デジタルライセンスデータをメモリに独自の方法で保存するのではなく、ファイル構成上に保存でき、また、デジタルライセンスデータの保存や検索、その他の管理

操作用ＡＰＩに公開され普及しているＡＰＩを提供できる。

【００５８】

次に、本発明の実施の形態１におけるセキュアコンテナを介して、デジタルデータ（コンテンツ）をある送信元（ソース）から送信先（シンク）に転送する方法の一例を、図３から図５を用いて説明する。

【００５９】

ソースからシンクへセキュアコンテナ５００を介したコンテンツ転送時のトランスコード処理において、４個のデータセットを定義する。４個のデータセットとは、コンテンツ（対応する鍵で暗号化されたもの）９０１と、コンテンツを暗号化するための鍵（ライセンスの一部）と、セキュアコンテナ５００とシンク間のセキュアなチャンネルで使用されるセッション鍵と、セキュアコンテナ５００内で制御操作を行う際に使用され、各鍵に対応した命令セット（ライセンスの一部）である。なお、これらのデータセットは、ソースまたはシンクからセキュアコンテナ５００へ通知されるが、通知するタイミングや通信手段は、同一である必要はなく、異なるパスで転送可能である。

【００６０】

ソースからシンクへのコンテンツの転送処理は、次の６つの段階に分けられる。ソースが、直接または間接的にコンテンツに関連付けられた鍵で暗号化されコンテンツ９０１を格納している段階（ａ）と、暗号化されたコンテンツをソースからセキュアコンテナへ転送する段階（ｂ）と、ソースからセキュアコンテナへ命令セットを転送する段階（ｃ）と、セキュアコンテナとシンクの間でセキュアなデータ通路を確立する段階（ｄ）と、シンクからセキュアコンテナへ命令セットを転送する段階（ｅ）と、コンテンツに関連付けられた鍵を用いてコンテンツ９０１を復号化し、トランスコード処理した後に、前記セキュアなデータ通路を通して転送する段階（ｆ）とである。

【００６１】

図３は、本発明の実施の形態１におけるセキュアコンテナ内での、前述した段階（ｆ）のトランスコード処理の概要を示している。

【００６２】

セキュアコンテナ５００は、暗号化されたコンテンツ９０１を入力とし、トランスコード処理９０２を実行して、復号した後で新しく暗号化した形式（トランスコード）９０８か、暗号化されていない形式９０９に変換し、シンクに出力する。このトランスコード処理９０２は、復号化９０３と暗号化９０４とから構成されており、暗号化されたコンテンツ９０１は、関連する復号化の鍵９０５とユーセッジルール９０６を用いて復号化され、更に、関連するユーセッジルール９０６で指定されている場合に、付加的な暗号化を行う。

【００６３】

図４は、本発明の実施の形態１におけるセキュアコンテナの、トランスコード処理の流れの一例を示すフローチャートである。

【００６４】

まず、セッションマネージャ５０２が、Ｉ／Ｏポート５０１を介して暗号化されたコンテンツをソースから受け取る（１００１）。

【００６５】

ライセンス管理エンジン５０６は、受け取ったコンテンツに関連付けられたライセンスデータをメモリ５０４から取得し、取得したライセンスデータをユーセッジルール適用部５０５に通知する。ユーセッジルール適用部５０５は、通知されたライセンスデータに基づいてユーセッジルールを決定し、この決定したユーセッジルールを適用して、復号化が必要か否か判定する（１００２）。

【００６６】

復号化が必要である場合（１００２がＹｅｓ）、暗号エンジン５０７は、ライセンスデータに基づいた復号化の鍵を用いて、暗号化されたコンテンツを復号化する（１００３）。復号化が必要でない場合（１００２がＮｏ）、復号化を行わずに、ステップ１００４に遷移する。

【００６７】

次に、ユーセッジルール適用部５０５は、先ほど決定したユーセッジルールを適用して、暗号化が必要か否かを判定する（１００４）。

【００６８】

暗号化が必要である場合（１００４がＹｅｓ）、暗号エンジン５０７は、セッ

ション鍵を用いてコンテンツを暗号化し（１００５）、セッションマネージャ５０２は、トランスコードされたコンテンツ（再暗号化されたコンテンツ）を、Ｉ／Ｏポート５０１を介してシンクに出力する（１００６）。暗号化が必要でない場合（１００４がＮｏ）、セッションマネージャ５０２は、復号化したコンテンツをそのまま、Ｉ／Ｏポート５０１を介してシンクに出力する（１００７）。

【００６９】

図５は、本発明の実施の形態１におけるセキュアコンテナの、トランスコード処理の流れの別の一例を示すフローチャートである。ここでは、ステップ１２０５で、処理対象のコンテンツを最後までトランスコード処理を行ったか否かを判断し、処理を継続する場合には（１２０５がＮＯ）、ステップ１２０２に戻り、トランスコードを繰り返し処理する。これにより、ストリーミングや周期的なコンテンツを扱ってトランスコードを行うことが可能となる。

【００７０】

なお、セキュアコンテナ５００とシンク間のセキュアな接続（ｄ）をディフィ・ヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）鍵交換方式を利用して確立することにより、公開されて普及している方法を用いてセキュアな接続を確立できる。

【００７１】

また、シンクへの転送の段階（ｆ）での命令セット（ユーセッジルール）に、シンクへの転送に使用するセキュアなデータ通路で用いられる暗号化の強度を記述する制御命令を含むことができる。これにより、制御命令で暗号化の強度（つまり、セキュアコンテナ（５００）とシンク間のセキュアなチャネルの強度）を管理することが可能となり、データ通路の種類に応じてより柔軟に安全性を向上することができる。

【００７２】

また、シンクへの転送の段階（ｆ）での命令セットに、シンクへの転送に使用するセキュアなデータ通路が有効である期間を示す制御命令を含むことができる。これにより、暗号化（セキュアコンテナ（５００）とシンク間のセキュアなチャネル）を管理するこの制御命令は、ステップ１００４における暗号化が可能な期間を規定することが可能となる。その結果、顧客が、購買期間中に（放送デー

タなどを）個人用にコピー保存したり、データを計画利用できたりする購買システムを確立することができる。

【００７３】

また、シンクへの転送の段階（ｆ）での命令セットに、データの複製をシンクにいくつ送信するかを示す制御命令を含むことができる。これにより、暗号化（セキュアコンテナとシンク間のセキュアなチャネル）を管理する制御命令は、送信可能なコピー回数を規定することが可能となり、データのバックアップや共有で使用する際に有効な回数を制限管理することができる。

【００７４】

また、シンクへの転送の段階（ｆ）での命令セットに、段階（ｃ）でソースから転送された命令セットの一部または全体を含めることができる。これにより、ソースからセキュアコンテナに送られた制御命令を追加することが可能となり、ソースがセキュリティ要件を規定できるなどの効果がある。ただし、ライセンスや鍵に付随する命令セットに定義されているデフォルト要件が弱められることはない。

【００７５】

また、シンクへの転送の段階（ｆ）での命令セットに、データがシンクに送信されるより事前に、シンクが適合すべき要求事項を示す制御命令を含むことができる。これにより、暗号化（セキュアコンテナとシンク間のセキュアなチャネル）を管理する制御命令は、シンクに対する要件を規定することが可能となり、その結果、ソースがシンクに要件を指示することが出来る。例えば、シンクは購入するのに高額なデータに対してはユーザによる確認といった一定のセキュリティ基準に従わなければならないなどの要件を指定できる。

【００７６】

また、セキュアコンテナとシンク間のセキュアな接続（ｄ）をＣＰＲＭ（Ｃｏｎｔｅｎｔｓ　Ｐｒｏｔｅｃｔｉｏｎ　ｏｆ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ、記録可能メディア用コンテンツ保護技術）を利用して確立することができる。ＣＰＲＭを利用することにより、ＳＤカードなど、ＣＰＲＭに対応するあらゆる環境でシステムを利用できる。

【００７７】

また、ソースからセキュアコンテナへの命令セットの転送の段階（ｃ）を行わなくてもよい。これにより、ソースが単に簡素な記憶装置、或いは記憶メディアである場合にも適用することができる。

【００７８】

次に、本発明の実施の形態１におけるセキュアコンテナを介して、再暗号化を適用した、デジタルデータ（コンテンツ）をある送信元（ソース）から送信先（シンク）に転送する方法の一例について、図６から図８を用いて説明する。

【００７９】

ソースからシンクへセキュアコンテナ５００を介したコンテンツ転送時の再暗号化処理において、３個のデータセットを定義する。３個のデータセットとは、コンテンツ（対応する鍵で暗号化されたもの）１４０１と、コンテンツを暗号化に使用する鍵１４０７と、セキュアコンテナ５００内で制御操作を行う際にしようされる命令セットである。なお、これらのデータセットは、ソースからセキュアコンテナ５００へ通知されるが、通知するタイミングや通信手段は、同一である必要はなく、異なるパスで転送可能である。また、セキュアコンテナ５００は、これらのデータセットを利用して再暗号化を行い、この再暗号化処理では、シンクに対応付けられた特定の鍵を用いて再暗号化を行うため、コンテンツを復号できるのは対応するシンクのみとなる。

【００８０】

ソースからシンクへの再暗号化を適用したコンテンツの転送処理は、次の５つの段階に分けられる。ソースが、コンテンツに関連付けられたある鍵を用いて対応するコンテンツを暗号化する段階（ａ）と、暗号化されたコンテンツ１４０１をソースからセキュアコンテナに転送する段階（ｂ）と、段階（ａ）で暗号化に使用した鍵をソースからセキュアコンテナへ転送する段階（ｃ）と、ソースからセキュアコンテナへ命令セットを転送する段階（ｄ）と、コンテンツに関連付けられた鍵を用いてコンテンツ１４０１を復号化し、シンクに関連付けられたある鍵を用いてコンテンツを再暗号化する段階（ｅ）とである。なお、復号化と再暗号化の段階（ｅ）は、セキュアコンテナが保持している命令セットによって制御

される。

【００８１】

図６は、本発明の実施の形態１におけるセキュアコンテナ内での、前述した段階（ｅ）の再暗号化処理の概要を示している。セキュアコンテナ５００は、暗号化されたコンテンツ１４０１を受け取り、再暗号化処理１４０２を実行して、再暗号化されたコンテンツ１４０８を出力する。この再暗号化処理１４０２は、復号化１４０３と暗号化１４０４とから構成されており、ライセンスに関連つけられた鍵（復号化の鍵１４０５）で暗号化されたコンテンツ１４０１がセキュアコンテナ５００に入力され、復号化の鍵１４０５を用いて復号化される。その後、関連するユーセッジルール１４０６を適用して、復号化されたコンテンツは、ライセンスに関連つけられた暗号化の鍵１４０７を用いて再暗号化を行い、再暗号化されたコンテンツを出力する。

【００８２】

図７は、本発明の実施の形態１におけるセキュアコンテナの、再暗号化処理の流れの一例を示すフローチャートである。

【００８３】

まず、セッションマネージャ５０２が、Ｉ／Ｏポート５０１を介して暗号化されたコンテンツをソースから受け取り、メモリ５０４に保持している（１５０１）。

【００８４】

ライセンス管理エンジン５０６は、コンテンツに関連付けられたライセンスデータをメモリ５０４から取得し、取得したライセンスをユーセッジルール適用部５０５に通知する。ユーセッジルール適用部５０５は、通知されたライセンスに基づいてユーセッジルールを決定し、この決定したユーセッジルールを適用して、再暗号化が許可されるか否かを判定する（１５０２）。

【００８５】

再暗号化が許可されない場合（１５０２がＮｏ）、処理を終了する。一方、再暗号化が許可される場合（１５０２がＹｅｓ）、暗号化エンジン５０７は、復号化の鍵を用いて、暗号化されたコンテンツを復号化する（１５０３）。

【００８６】

暗号化エンジン５０７は、関連するユーセッジルールを適用して、復号化されたコンテンツを、ライセンスに関連付けられた暗号化の鍵を用いて再暗号化を行い（１５０４）、セッションマネージャ５０２は、再暗号化されたコンテンツをＩ／Ｏポート５０１を介して出力する（１５０５）。

【００８７】

図８は、本発明の実施の形態１におけるセキュアコンテナの、周期的なコンテンツの再暗号化処理の流れの一例を示すフローチャートである。まず、セッションマネージャ５０２が、Ｉ／Ｏポート５０１を介して暗号化されたコンテンツをソースから受け取り、メモリ５０４に保持しているものとする。

【００８８】

ライセンス管理エンジン５０６は、コンテンツに関連付けられたライセンスデータをメモリ５０４から取得し、取得したライセンスデータをユーセッジルール適用部５０５に通知する。ユーセッジルール適用部５０５は、通知されたライセンスデータに基づいてユーセッジルールを決定し、この決定したユーセッジルールを適用して、再暗号化が許可されるか否かを判定する（１６０１）。

【００８９】

再暗号化が許可されない場合（１６０１がＮｏ）、処理を終了する。一方、再暗号化が許可される場合（１６０１がＹｅｓ）、暗号化エンジン５０７は、メモリ５０４から暗号化されたコンテンツの一部を読み込み、復号化の鍵を用いて、読み込んだ暗号化されたコンテンツを復号化する（１６０２）。

【００９０】

暗号化エンジン５０７は、関連するユーセッジルールを適用して、復号化されたコンテンツの一部を再暗号化し、セッションマネージャ５０２は、再暗号化されたコンテンツをＩ／Ｏポート５０１を介して出力する（１６０３）。

【００９１】

次に、ユーセッジルール適用部５０５は、ユーセッジルールを適用して、コンテンツの次の一部の再暗号化が許可されるか否かを判定する（１６０４）。コンテンツの次の再暗号化が許可されれば（１６０４がＮｏ）、ステップ１６０２に

遷移し、処理を継続する。一方、再暗号化が許可されない場合（１６０４がＹｅｓ）、処理を終了する。なお、ステップ１６０４において、コンテンツの最後まで処理が完了した場合も、再暗号化が許可されないと判断し、処理を終了する。

【００９２】

以上により、顧客がコンテンツを個別化するこが可能となり、他人にコンテンツを利用されることがない。また、コンテンツを再暗号化処理で匿名化することもできる。

【００９３】

また、段階（ｅ）での命令セット（ユーセッジルール）に、再暗号化に許される計算時間を示す制御命令を含むことができる。これにより、再暗号化を管理する制御命令は、再暗号化可能期間を規定することが可能となる。その結果、顧客が、購買期間中に（放送データなどを）個人用にコピー保存することが可能な購買システムを確立することができる。

【００９４】

また、段階（ｅ）での命令セットに、データの再暗号化された複製をいくつ生成するかを示す制御命令を含むことができる。これにより、再暗号化を管理する制御命令は、コピー回数を規定することが可能となり、データのバックアップや共有で使用する際に有効な回数を制限管理することができる。更に、コンテンツが顧客に対応付けられているので、監視や監査が可能である。

【００９５】

また、段階（ｅ）での命令セットは、再暗号化が許されるより事前に、シンクが適合すべき要求事項を示す制御命令を含むことができる。これにより、再暗号化を管理する制御命令は、シンクに対する要件を規定することが可能となり、その結果、ソースはシンクに要件を指示することが出来る。例えば、シンクは購入するのに高額なデータに対しては一定のセキュリティ基準に従わなければならないなどの要件を指定できる。

【００９６】

また、段階（ｅ）での命令セットは、段階（ｃ）で転送される命令を含むことができる。再暗号化されるデータの複製の個数を規定する制御命令は、（シンク

にある）内蔵型の制御命令ではなく、ソースから転送されなければならない。命令セットに含めることによって、これら制御命令を有効に規定できる。

【００９７】

また、段階（ｅ）は、少なくとも部分的にソースに置かれている命令セットによって制御されることが可能である。この場合、制御命令はソースに存在し、暗号化はソースで行われる。その結果、データ製作者や所有者に対応しているソースが、再暗号化の処理を完全に制御できるという効果がある。また、再暗号化を管理する制御命令がシンクに存在する場合、シンクが独立して再暗号化を行うことが出来るという効果がある。

【００９８】

次に、本発明の実施の形態１におけるセキュアコンテナにおいて、ライセンスの存在を証明する方法の一例を、図９と図１０を用いて説明する。なお、セキュアコンテナは、シンク内に実装されものとし、このシンクに格納されたライセンスの詳細情報をソースに与えることなしに、ライセンスの存在を証明する方法である。

【００９９】

ソースが、シンクのライセンスプールの中にあるライセンスが存在すること示す証明を受け取りたい場合、ソースは、セキュアなチャネルを利用して、シンクに証明書発行の要求を出さなければならない。シンク（セキュアコンテナ）は、ソースからシンクに送られた要求（チャレンジ）を考慮に入れて証明書を生成する。生成された証明書は、セキュアなチャネルを介してソースに送られる。

【０１００】

チャレンジは、認証技術を持つプロトコルの一形態であるチャレンジーレスポンス型プロトコルで用いられるものである。クライアント（シンク）のＤＲＭシステムは、ライセンスに埋め込まれた秘密鍵でチャレンジに署名を行い、サーバー（ソース）は、ライセンスの一部である公開鍵でこの署名を確認する。これにより、ＤＲＭシステムがライセンスを保持し、正しい証明書の要求に答えているかどうかを、サーバは、確認することができる。例えば、利用者は、自身の秘密のコード（チャレンジ）をスマートカードに入力し、あるシステムにログインす

る新しいコード（レスポンス）を得る、といったものである。

【０１０１】

ライセンスの存在を証明する処理は、次の６つの段階に分けられる。ソースとシンクの相互認証を行う段階（ａ）と、ソースとシンクの間にセキュアなデータ通路を確立する段階（ｂ）と、ライセンスの存在証明の要求であるチャレンジをシンクに転送する段階（ｃ）と、シンクにおいてチャレンジとライセンスのデータを用いて固有の証明を生成する段階（ｄ）と、生成した固有の証明をソースに転送する段階（ｅ）と、ソースにおいて取得した証明を検証する段階（ｆ）とである。

【０１０２】

図９は、本発明の実施の形態１におけるセキュアコンテナ内での、前述した段階（ｄ）のライセンスの存在の証明を生成する処理の概要を示している。セキュアコンテナ５００は、ライセンスの証明を要求するセッションでチャレンジを受け取り、ライセンスの存在を証明する処理１８０１を実行して、生成した証明書１８０４を出力する。このライセンスの存在を証明する処理１８０１は、証明書を生成する処理１８０２と、データを追加する処理１８０３とから構成されており、ライセンスの証明を要求するセッションでチャレンジがセキュアコンテナ５００に通知され、ライセンスプール１８０６からライセンスを取得し、通知されたチャレンジを用いて証明書を作成する。その後、関連するユーセッジルールを適用して、要求があるなら、ライセンスからのデータや、メタデータを、証明書に追加する。また、必要であれば、新しく生成された証明書は、セッション鍵を用いて暗号化され、この証明書１８０４を出力する。

【０１０３】

この証明もしくは証明書とは、ライセンスを示す必要がある場合に、ライセンスの内容まで開示すると不正利用や改ざんされる恐れがあるので、内容を示す必要がない場合に、ただライセンスを保持しているという保証を示すためのものである。例えば、電子チケットでは、有効なチケットを持っていることが重要なのであって、暗号を用いていた中身をすべて開示される必要がない。

【０１０４】

また、メタデータとは、ライセンスや証明書に直接は関係のない情報である。例えば、映画館用の電子チケットにおいては座席番号やドリンクサービスなどの付加的な情報を示しており、これだけに限定されない。

【０１０５】

図１０は、本発明の実施の形態１におけるセキュアコンテナの、ライセンスの存在の証明を生成する処理の流れの一例を示すフローチャートである。まず、セッションマネージャ５０２が、Ｉ／Ｏポート５０１を介してライセンスの証明を要求するチャンレンジをソースから受け取り、処理を開始する。

【０１０６】

ライセンス管理エンジン５０６は、対応するライセンスをメモリ５０４（ライセンスプール）から取得し、取得したライセンスデータをユーセッジルール適用部５０５に通知する。ユーセッジルール適用部５０５は、通知されたライセンスデータに基づいてユーセッジルールを決定し、この決定したユーセッジルールを適用して、チャレンジの要求が有効か無効かを判定する（１９０１）。

【０１０７】

要求が無効である場合（１９０１がＮｏ）、処理を終了する。なお、対応するライセンスがメモリ５０４に格納されていない場合も、要求が無効であるとして、処理を終了する。一方、要求が有効である場合（１９０１がＹｅｓ）、暗号エンジン５０７は、ライセンスとチャレンジを用いて、証明書を生成する（１９０２）。

【０１０８】

ユーセッジルール適用部５０５は、ユーセッジルールを適用して、証明書に付加的なデータの追加が必要か否かを判定する（１９０３）。付加的なデータの追加が必要な場合（１９０３がＹｅｓ）、ライセンス管理エンジン５０６は、ライセンスから付加されるデータを抽出し、証明書にデータを付加する（１９０４）。

【０１０９】

ユーセッジルール適用部５０５は、ユーセッジルールを適用して、証明書に暗号化が必要か否かを判定する（１９０５）。暗号化が必要な場合（１９０５がＹ

ｅｓ）、暗号化エンジン５０７は、セッション鍵を用いて証明書の暗号化を行う（１９０６）。最後に、セッションマネージャ５０２は、生成した証明書をＩ／Ｏポート５０１を介して出力する。

【０１１０】

なお、要求がユーセッジルールに基づいて有効か否かとは、例えば、電子チケットを利用する場合に、その電子チケットの有効期限や利用回数がユーセッジルールに書込まれていて、適合していれば利用可能な電子チケットとして有効であるというものである。この場合、ユーセッジルールを用いて、ライセンスが有効であるかないかを判定したが、ライセンスのデータファイルの名前や作成期日をチェックするなど、システムや外部のものが判定してもよい。

【０１１１】

また、付加的なデータとは、例えば、映画館用の電子チケットにおいて、映画鑑賞後のコメントをアンケートする人を選ぶためのマーキングなどであり、これだけに限定されない。

【０１１２】

また、ライセンスに固有な証明書を発行する利点は、シンクがライセンスの詳細情報をソースに送る必要がない点である。また、この証明書は、ライセンスがｅチケットの代わりになる電子チケットシステムでも利用可能である。

【０１１３】

また、セキュアコンテナとシンク間のセキュアな接続（ｂ）がディフィ・ヘルマン鍵交換方式を利用して確立することにより、公開され普及している方法によってセキュアな接続を確立できる。

【０１１４】

また、セキュアコンテナとシンク間のセキュアな接続（ｂ）をＣＰＲＭを利用して確立することができる。ＣＰＲＭを利用することにより、ＳＤカードなど、ＣＰＲＭに対応するあらゆる環境でシステムを利用できる。

【０１１５】

また、証明を生成する段階（ｄ）は、命令セットによって制御される。これにより、証明書の生成を管理する制御命令は、証明書の生成方法に影響を与えるこ

とが可能となり、ライセンス発行者が証明書の生成方法を制御できる。

【０１１６】

また、証明を生成する段階（ｄ）で、片方向ハッシュ関数を利用するとことが可能であり、これにより、暗号化されたセキュアな証明書を生成できる。

【０１１７】

また、証明を生成する段階（ｄ）で、チャレンジと証明を、ソースの公開鍵を用いて暗号化することができる。これにより、ソースとセキュアコンテナ間の接続をセキュアにする必要がないという利点がある。この場合、セキュリティは公開鍵方式で実現される。ここで、ソースの公開鍵は、ライセンスの一部として組み込まれる可能性がある。

【０１１８】

また、証明を生成する段階（ｄ）で、証明をソースに転送する前に、証明はライセンスに含まれる鍵を用いて暗号化することができる。これにより、ライセンス発行者や許可された第三者のみが、証明を復号できる。更に、ソースが証明書を復号できるのであれば、そのソースは許可されたものであると考えられることから、ソースが自身の認証をセキュアコンテナに対し行う必要がなくなる。

【０１１９】

また、証明をソースに転送する段階（ｅ）で、証明は、ライセンスに含まれる付加的なデータとともに、ソースに転送することができる。これにより、電子チケットを実現することが可能となる。

【０１２０】

また、ライセンスに含まれる付加データを証明に添付して、この証明をソースに転送する前に、転送する証明や付加データ、またはこの両方を、ライセンスに含まれる鍵（セッション鍵）によって暗号化することができる。これにより、電子チケットを実現することが可能となる。

【０１２１】

また、命令セットに、ライセンスに含まれるどのデータが、証明に付加されるべきかという情報を含めることができる。これにより、証明の生成を管理する制御命令に、ライセンスに含まれるどのデータを証明に添付すべきかを示す情報を

含めることが可能となり、コンテンツの有効期限や有効地域情報といった、ライセンスに付随するメタデータの特定のものを証明に添付することができる。

【０１２２】

また、命令セットに、ランダムデータを含めることが可能となる。つまり、ランダムデータを証明に添付した後、暗号化を行う。この結果をランダムなデータにみせかけ、先に送付されている他のライセンス証明との関連性なくすことができるという利点が生まれる。

【０１２３】

次に、本発明の実施の形態１におけるセキュアコンテナにおいて、ライセンス状態情報の変更方法の一例を、図１１と図１２を用いて説明する。ライセンス状態情報は、必要であればライセンスに割り当てられるか、ライセンスの中に組み込まれる。ライセンス状態情報を変更したい場合、まず、ソースとセキュアコンテナ間の相互認証を行い、認証が成功することにより、セキュアなチャネルが確立される。次に、ソースからセキュアコンテナに、ライセンス状態情報の変更の要求が送付され、セキュアコンテナは、受け取った要求に従って処理を行う。ライセンス状態情報の変更が成功すれば、セキュアコンテナは、変更の証明をソースに送付する。ソースでは、送付された証明を用いて、要求した変更の結果を確認することができる。なお、セキュアコンテナは、シンク内に実装されものとする。

【０１２４】

ライセンス状態情報の変更処理は、次の７つの段階に分けられる。ソースとシンクの相互認証を行う段階（ａ）と、ソースとシンクの間にセキュアなデータ通路を確立する段階（ｂ）と、ライセンス状態情報を変更する要求とともにチャレンジをシンクに転送する段階（ｃ）と、シンクにおいて要求された変更をライセンスに行う段階（ｄ）と、ソースにおいてチャレンジとライセンスのデータを用いて固有の証明を生成する段階（ｅ）と、生成した固有の証明をソースに転送する段階（ｆ）と、ソースにおいて取得した証明を検証する段階（ｇ）とである。

【０１２５】

図１１は、本発明の実施の形態１におけるセキュアコンテナ内での、ライセン

スの存在の証明を生成し、さらにライセンスを変更する処理の概要を示している。セキュアコンテナ５００は、ライセンスの証明を要求するセッションでチャレンジを受け取り、ライセンスの存在の証明を生成／ライセンスを変更する処理２１０１を実行して、生成した証明書２１０５を出力する。このライセンスの存在の証明を生成／ライセンスを変更する処理２１０１は、ライセンスの状態情報を変更する処理２１０２と、証明書を生成する処理２１０３と、データを追加する処理２１０４とから構成されており、ライセンス状態情報の変更の要求とチャレンジがセキュアコンテナ５００に通知され、ライセンスプール２１０６からからライセンスを取得し、通知された変更の要求に従ってライセンスデータを修正する。ライセンスプール２１０６に格納されているライセンスを、この修正されたライセンスに更新し、チャレンジを用いて証明書を作成する。その後、関連するユーセッジルールを適用して、要求があるなら、ライセンスからのデータや、メタデータを、証明書に追加する。また、必要であれば、新しく生成された証明書は、セッション鍵を用いて暗号化され、この証明書２１０５を出力する。なお、ユーセッジルールは、出力されるデータパケット（証明書２１０５を示す）にも適用される。

【０１２６】

図１２は、本発明の実施の形態１におけるセキュアコンテナの、ライセンスを変更し、さらにライセンスの存在の証明を生成する処理の流れの一例を示すフローチャートである。まず、セッションマネージャ５０２が、Ｉ／Ｏポート５０１を介して、ライセンス状態情報の変更の要求と、ライセンスの証明を要求するチャンレジをソースから受け取り、処理を開始する。

【０１２７】

ライセンス管理エンジン５０６は、対応するライセンスをメモリ５０４（ライセンスプール）から取得し、取得したライセンスデータをユーセッジルール適用部５０５に通知する。ユーセッジルール適用部５０５は、通知されたライセンスデータに基づいてユーセッジルールを決定し、この決定したユーセッジルールを適用して、チャレンジの要求が有効か無効かを判定する（２２０１）。

【０１２８】

要求が無効である場合（２２０１がＮｏ）、処理を終了する。なお、対応するライセンスがメモリ５０４に格納されていない場合も、要求が無効であるとして、処理を終了する。一方、要求が有効である場合（２２０１がＹｅｓ）、ライセンス管理エンジン５０６は、受け取ったライセンス状態情報の変更の要求に基づき、ライセンスの状態情報を変更し（２２０２）、メモリ５０４（ライセンスプール）に格納されているライセンスを、変更したライセンスに更新する（２２０３）。

【０１２９】

次に、暗号エンジン５０７は、ライセンスとチャレンジを用いて、証明書を生成する（２２０４）。

【０１３０】

ユーセッジルール適用部５０５は、ユーセッジルールを適用して、証明書に付加的なデータの追加が必要か否かを判定する（２２０５）。付加的なデータの追加が必要な場合（２２０５がＹｅｓ）、ライセンス管理データ５０６は、ライセンスから付加されるデータを抽出し、証明書にデータを付加する（２２０６）。なお、付加データを追加する必要がなければ（２２０５がＮｏ）、データ追加は行わない。

【０１３１】

ユーセッジルール適用部５０５は、ユーセッジルールを適用して、証明書に暗号化が必要か否かを判定する（２２０７）。暗号化が必要な場合（２２０７がＹｅｓ）、暗号化エンジン５０７は、セッション鍵を用いて証明書の暗号化を行う（２２０８）。最後に、セッションマネージャ５０２は、生成した証明書をＩ／Ｏポート５０１を介して出力する。

【０１３２】

なお、ライセンスの変更の例としては、年毎のライセンスや会員制のサービスなどで、年間会費を支払うことにより、ライセンスの有効性が延長されるよう変更する場合である。具体例として、ソフトウェアライセンスやオンラインマガジンの予約購読などに用いることができる。他の例として、複数の電子チケットの場合、有効期限内に１０回利用できる電車の回数券に適用されると、残り利用回

数を減少したり、期限になると無効にしたりする変更を行うことができる。

【０１３３】

この方法の利点は、ライセンス状態情報の変更で、双方向、あるいは複数の電子チケットを実現できる点とライセンスに対応するデジタルデータの使用を制限できる点である。以下に説明を記す。

【０１３４】

ライセンスの変更を許可するシステムでは、システム側での管理外でライセンスが変更される可能性が高くなり、セキュリティ上の危険が増加する。そのため、ライセンスに一つ以上の変更できる情報を持たせ、ライセンスの変更方法や、有効な変更の範囲を、ユーセッジルールに記述することにより、セキュリティ上の危険を減少し、安全にライセンスの変更を可能とすることができる。

【０１３５】

ライセンスの状態の例としては、往復チケットで、一つ目の状態は「往路」であり、二つ目の状態は「復路」、というものが挙げられる。往復チケットの状態は、「復路」の後は、自動的に「無効」となる。ライセンスの状態変更のみ許可するのであれば、コンテンツを復号化する鍵などを保護でき、セキュリティを向上させることができる。また、他の例として、ある映画コンテンツの再生許可回数や再生許可時間という状態をライセンスに定めておく。映画コンテンツのデジタルデータが利用されると、ライセンスに含まれる状態情報が、定められた状態まではアップデートされる。回数や時間の定められた状態に達すると、ライセンスは「無効」の状態になり、デジタルデータの利用ができなくなる。

【０１３６】

また、セキュアコンテナとシンク間のセキュアな接続（ｂ）がディフィ・ヘルマン鍵交換方式を利用して確立することにより、公開され普及している方法によってセキュアな接続を確立できる。

【０１３７】

また、セキュアコンテナとシンク間のセキュアな接続（ｂ）をＣＰＲＭを利用して確立することができる。ＣＰＲＭを利用することにより、ＳＤカードなど、ＣＰＲＭに対応するあらゆる環境でシステムを利用できる。

【０１３８】

また、証明を生成する段階（ｅ）は、命令セットによって制御される。これにより、証明書の生成を管理する制御命令は、証明書の生成方法に影響を与えることが可能となり、ライセンス発行者が証明書の生成方法を制御できる。

【０１３９】

また、証明を生成する段階（ｅ）で、片方向ハッシュ関数を利用することが可能であり、これにより、暗号化されたセキュアな証明書を生成できる。

【０１４０】

また、証明を生成する段階（ｅ）で、チャレンジと証明を、ソースの公開鍵を用いて暗号化することができる。これにより、ソースとセキュアコンテナ間の接続をセキュアにする必要がないという利点がある。この場合、セキュリティは公開鍵方式で実現される。ここで、ソースの公開鍵は、ライセンスの一部として組み込まれる可能性がある。

【０１４１】

また、証明を生成する段階（ｅ）で、証明をソースに転送する前に、証明はライセンスに含まれる鍵を用いて暗号化することができる。これにより、ライセンス発行者や許可された第三者のみが、証明を復号できる。更に、ソースが証明書を復号できるのであれば、そのソースは許可されたものであると考えられることから、ソースが自身の認証をセキュアコンテナに対し行う必要がなくなる。

【０１４２】

また、証明をソースに転送する段階（ｆ）で、証明は、ライセンスに含まれる付加的なデータとともに、ソースに転送することができる。これにより、電子チケットを実現することができる。

【０１４３】

また、ライセンスに含まれる付加データを証明に添付して、この証明をソースに転送する前に、転送する証明や付加データ、またはこの両方を、ライセンスに含まれる鍵（セッション鍵）によって暗号化することができる。これにより、電子チケットを実現することが可能となる。

【０１４４】

また、命令セットに、ライセンスに含まれるどのデータが、証明に付加されるべきかという情報を含めることができる。これにより、ライセンスに付随するメタデータの特定のものを証明に添付することができる。

【０１４５】

また、命令セットに、ランダムデータを含めることが可能となる。つまり、短ダムデータを証明に添付した後、暗号化を行う。この結果をランダムデータにみせかけ、先に送付されている他のライセンス証明との関連性なくすことができるという利点が生まれる。

【０１４６】

図１５は、本発明の実施の形態１におけるシステムの概要を示す図である。サーバであるコンテンツプロバイダー３００（以下、サーバと記載する）と、ＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔ　Ｍａｎａｇｅｍｅｎｔ）装置３０８を備えるクライアント３１８との、少なくとも２つの構成要素から構成されている。また、ＰＣ３１９を更に備え、サーバから取得するコンテンツを格納するために用いられてもよい。サーバ３００とクライアント３１８は、ネットワークを介して接続可能であり、クライアント３１８は、サーバ３００からネットワーク経由で取得したコンテンツに対し、記憶保持や再生などの処理を行う装置である。サーバ３００内のコンテンツ記憶装置３０１よりコンテンツを取得する際、サーバ３００は、コンテンツに関連するライセンス（鍵）３０３を用いて配信対象のコンテンツを暗号化する（３０２）。このライセンス３０３は、ＤＲＭ装置３０８とサーバ３００間のセッションで定義されるセッション鍵３０４を用いて暗号化され（３０５）、この後、暗号化されたライセンスは、ＤＲＭ装置３０８に通知される。ＤＲＭ装置３０８は、暗号化されたライセンスを受け取り、セッション鍵３１１を用いて復号化し（３０９）、復号化されたライセンスをライセンス記憶装置３１０に格納する。なお、セッション鍵で復号化するとしたが、暗号化されたままでライセンス記憶装置３１０に格納してもよい。一方、サーバ３００から取得したコンテンツは、クライアント３１８内のコンテンツ記憶装置３１７に格納される。なお、ＰＣ３１９内のコンテンツ記憶装置３０７に格納してもよい。このサーバ３００から取得したコンテンツを再生するために、再生対象のコンテン

ツをＤＲＭ装置３０８に通知し、ライセンス記憶装置３１０に格納した関連するライセンスを用いて、コンテンツを復号化する（３１２）。なお、復号化に加えて再び暗号化するトランスコード（３１２）を適用することができる。このトランスコードには、ＤＲＭ装置３０８とクライアント３１８間のセッションで定義されるセッション鍵３１３を用いる。クライアント３１８は、ＤＲＭ装置３０８からコンテンツを受け取り、必要に応じてセッション鍵３１４を用いて復号化を行い、取得したコンテンツの再生処理などのメディア出力を実行する。

【０１４７】

ライセンス３０３は、ユーセッジルールや暗号部分を含んでいる。ライセンス鍵３０２は、ライセンス３０３の暗号に関する一部であり、ライセンス内に一つ以上含まれてもよい。

【０１４８】

クライアント３１８とは、エンドユーザのデバイスや、コンテンツを取り込むデバイスを指す。ＤＲＭ装置３０８とは、クライアント３１８に実装されるＤＲＭシステムであり、クライアント３１８内に固定されていても、着脱可能であってもよい。着脱可能であるものとして、ＤＲＭシステムを含むメモリカードが考えられる。

【０１４９】

セッション鍵は、セキュアな接続を保証するために暗号化と復号化に用いられる一時的な鍵である。セッション鍵は、接続のやり取りであるセッションが行われている期間と場所のみ有効である。

【０１５０】

図１６は、本発明の実施の形態１におけるの別のシステムの概要を示す図である。サーバであるコンテンツプロバイダー３００（以下、サーバと記載する）と、ＤＲＭ装置３０８を備えるクライアント３１８と、外部の記憶装置メディア４００との、少なくとも３つの構成要素から構成されている。前述した図１５と基本的には同じであるが、コンテンツデータは外部の記憶メディア４００（または外部の記憶デバイス）にのみ格納されることができる点が異なる。サーバ３００から取得したコンテンツを再生するには、再生対象のコンテンツを記憶メディア

４００からクライアント３１８のＤＲＭ装置３０８に通知し、ライセンス記憶装置３１０に格納した関連するライセンスを用いて、コンテンツを復号化する（３１２）。なお、復号化に加えて再び暗号化するトランスコード（３１２）を適用することができる。このトランスコードには、ＤＲＭ装置３０８とクライアント３１８間のセッションで定義されるセッション鍵３１３を用いる。クライアント３１８は、ＤＲＭ装置３０８からコンテンツを受け取り、必要に応じてセッション鍵３１４を用いて復号化を行い、取得したコンテンツの再生処理などのメディア出力を実行する。

【０１５１】

例えば、ユーザはカード型システムを利用して、オンラインでライセンスを購入することができる。購入を行う時は、認証確認を実行し、認証が無事完了した時点で、システムはライセンス発行者（サーバ３００）とのセキュアな接続を確立する。その後、要求されたライセンスデータを暗号化し、システムに送付する。システムは、暗号化されたライセンスデータを復号（３０９）し、それが有効なものであるかを確認した後、ライセンス記憶装置３１０に保存する。ライセンスを暗号化した状態で保存するという命令セット、つまりユーセッジルールがある場合は、システムに内蔵された固有のデバイス秘密鍵を使ってライセンスを暗号化した後、データをライセンス記憶装置３１０に保存する。

【０１５２】

ユーザが例えばオーディオコンテンツを再生したい場合、ＤＲＭ装置３０８は、まず認証を行い、認証が正常に終了すると、ユーザのクライアント再生デバイス（クライアント３１８）とのセキュアな接続を確立し、セッション鍵（３１３、３１４）を用意する。セッション鍵（３１３、３１４）が発行されると、該当するコンテンツはＤＲＭ装置３０８に送付される。ここでは、コンテンツは対応するライセンスに含まれる鍵で暗号化（３１２）され、セッション鍵で再び暗号化（３１２）された後、クライアントの再生デバイス（クライアント３１８）に転送される。ＤＲＭ装置３０８からクライアント３１８に送付されたコンテンツは、決められたセッション鍵３１４を使って復号された後、クライアントデータパス（３１５）を処理され、クライアント３１８のメディア出力（３１６）に送

付される。

【０１５３】

ライセンス付きのコンテンツを再暗号化し、再発行されたライセンスと対応付ける必要がある場合、コンテンツはクライアント３１８からＤＲＭ装置３０８に送られ、まず現行のライセンス鍵で復号され、再発行されたライセンス鍵で再び暗号化された後、クライアント３１８に返送される。この場合、オリジナルのライセンスに対応付けられている命令セット（ユーセッジルール）で再暗号化処理の制御と認可を行う。

【０１５４】

電子チケットサービスなどの目的で、ＤＲＭ装置にライセンスの存在証明の発行を、その権利を持ったものが要求した場合、本発明では、クライアントに存在証明以上のライセンスデータを送信する必要がない。クライアント或いは権利を持つ者がＤＲＭ装置との認証に成功すると、両者間にセキュアな接続が確立され、セッション鍵が決定される。権利を持つ者或いはクライアントがＤＲＭ装置に存在証明を要求すると、ＤＲＭ装置は証明を作成する。証明書にはオプションで付加データを含ませることが出来る。ライセンスに付随する制御命令セット、つまり利用条件は、ライセンスの存在が証明できれば、証明書の生成に影響を与えることができる。制御命令セットは、証明書発行要求ごとに異なる証明書を発行する、証明書はランダムな特質を持つ、などの要求を出し、証明書生成に影響を与えることが出来る。

【０１５５】

権利を持つ者が、複数の電子チケットを求めるなど、ライセンス状態データの変更を求める場合、その変更の制御命令が存在証明書の発行要求に組み込まれる。この制御命令には、該当するライセンスの状態情報にどのような変更を加えるべきかを定義している。ＤＲＭ装置は、要求された変更を実行し、アップデートされた状態データが追加されたライセンス証明を発行要求者に返す。

【０１５６】

（実施の形態２）

図２は、本発明の実施の形態２におけるセキュアコンテナの構成を示す機能ブ

ロック図である。

【０１５７】

セキュアコンテナ６００は、Ｉ／Ｏポート５０１と、セッションマネージャ５０２と、ライセンス管理エンジン５０６と、ユーセッジルール適用部５０５と、暗号エンジン５０７と、メモリ管理部５０３と、メモリ５０４とを備えている点は実施の形態１と同様だが、実施の形態２においては、デバイス依存鍵６０１と、ログ管理エンジン６０２とを追加している。

【０１５８】

本発明の実施の形態２において新規に追加された構成要素について説明する。

【０１５９】

デバイス依存鍵６０１は、システムに固有の鍵であって、暗号化と復号化のために、１つだけでなく複数個備えることが可能である。例えば、暗号エンジン５０７が、共通鍵暗号のアルゴリズムを用いてライセンスデータなどを暗号化および復号化する際に、このデバイス依存鍵６０１を使用する。デバイス依存鍵６０１は、デバイスごとに固有であって、予めデバイス内部に格納またはハードコードされている。また、デバイス依存鍵６０１のうち、利用者の情報を参照していない場合、匿名（ａｎｏｎｙｍｏｕｓ）の性質を持つという。このようにライセンスが匿名で格納されている場合、デバイス依存鍵または組込みの鍵が用いられる。

【０１６０】

ログ管理エンジン６０２は、セキュアコンテナで処理された状態の変化をログ情報として記録保持を行う。セッション上の通信トランザクションのログ情報や、暗号エンジン５０７での暗号や復号の処理や、その他のセキュリティに関する処理を、セッションマネージャ５０２から受け取り、ログ情報として記録保持する。

【０１６１】

以上により、システムに固有な鍵をコンテンツの暗号化に用いることが可能となり、データの盗聴や改ざんを防ぐ安全性をより強化できる。更に、セキュアコンテナやそこに保存されているデジタルライセンスデータが改ざんや乱用を受け

た場合、システム制作者や許可された第三者がそれを認識できるようになる。

【０１６２】

本発明の実施の形態２におけるセキュアコンテナにおいて、ライセンスを保存する方法の一例を、図１３と図１４を用いて説明する。セキュアコンテナとソース間の相互認証を行い、認証が成功することにより、セキュアなチャネルが確立される。このセキュアなチャネルを介して受け取ったライセンスデータは、セキュアコンテナ内の内部メモリに保存される。なお、セキュアコンテナは、シンク内に実装されものとする。

【０１６３】

ライセンスを保存する処理は、次の４つの段階に分けられる。ソースとシンクの相互認証を行う段階（ａ）と、ソースとシンクの間にセキュアなデータ通路を確立する段階（ｂ）と、ライセンスをセキュアなデータ通路を通してソースからシンクに転送する段階（ｃ）と、シンクにおいてラインセンスを格納する段階（ｄ）とである。

【０１６４】

図１３は、本発明の実施の形態２におけるセキュアコンテナ内での、ライセンスを保存する処理の概要を示している。セキュアコンテナ５００は、暗号化されたライセンス受け取り、ライセンスを保存する処理２４０４を実行して、ライセンスをライセンスプールに格納する。このライセンスを保存する処理２４０４は、復号化２４０３と暗号化２４０４とから構成されており、暗号化されたライセンス２４０１がセキュアコンテナ５００に通知され、ソースとシンク間のセッション鍵を用いて復号化される。その後、ユーセッジルールを適用し、必要であるなら、復号化されたライセンスを再暗号化する。復号化もしくは再暗号化されたライセンスを、ライセンスプールに２４０５に格納する。

【０１６５】

図１４は、本発明の実施の形態２におけるセキュアコンテナの、ライセンスを保存する処理の流れの一例を示すフローチャートである。まず、セッションマネージャ５０２が、Ｉ／Ｏポート５０１を介して、暗号化されたライセンスを受け取り、処理を開始する。

【０１６６】

ライセンス管理エンジン５０６は、受け取ったライセンスがＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）固有であるか否かを判断する（２５０１）。ライセンスがＩＤ固有である場合（２５０１がＩＤ固有）、暗号エンジン５０７は、対応するＩＤを持つユーザの秘密鍵を用いて、ライセンスを復号化する（２５０２）。一方、ライセンスが匿名（ａｎｏｎｙｍｏｕｓ）である場合（２５０１が匿名）、暗号エンジン５０７は、デバイス依存の秘密鍵（デバイス依存鍵６０１）を用いて、ライセンスを復号化する（２５０３）。ライセンス管理エンジン５０６は、復号化したライセンスが有効か否かを判断し（２５０４）、有効でない場合（２５０４がＮｏ）、処理を終了する。

【０１６７】

ライセンス管理エンジン５０６は、復号化したライセンスをユーセッジルール適用部５０５に通知する。ユーセッジルール適用部５０５は、通知されたライセンスに基づいてユーセッジルールを決定し、この決定したユーセッジルールを適用して、ライセンスの暗号化が必要か否かを判定する（２５０５）。

【０１６８】

ライセンスは暗号化が必要な場合（２５０５がＹｅｓ）、暗号化エンジン５０７は、復号化されたライセンスを、デバイス依存の秘密鍵（デバイス依存鍵６０１）を用いて暗号化する（２５０６）。暗号化が必要でない場合（２５０５がＮｏ）、暗号化は行わない。暗号化管理エンジン５０６は、復号化されたライセンス又は再暗号化されたライセンスを、メモリ５０４（ライセンスプール）に格納する（２５０７）。

【０１６９】

なお、ＩＤ固有のライセンスとは、利用者の秘密鍵で暗号化されているライセンスであり、ライセンスプールに格納される。利用者の秘密鍵とは、パスワードなどの利用者に関連する情報を含んでいたり、システムの利用者の情報として登録されていたりする。しかし、暗号化に用いられる利用者の秘密鍵は、公開されず、ユーザ自身も、システムに格納されている鍵以外は複製を持つことができない。この秘密鍵は、コンテンツプロバイダーや、システムの製造者、認可された

第三者機関により与えられたり、デバイス内部で生成されたりする。

【０１７０】

一方で、暗号化に用いる鍵と復号化に用いる鍵が異なる公開鍵暗号を用いることもできる。公開鍵を採用する場合、暗号化に用いる公開鍵はデバイスから提供される。ただし、暗号化の鍵と関連はあるものの、暗号化の鍵のみでは復号化の鍵を、適当な時間内には計算することはできない。

【０１７１】

以上により、ライセンスをセキュアコンテナに保存する時に、ライセンスデータはソースからシンクへセキュアなデータ通路を介して転送され、シンクのメモリに安全に保存される。ライセンスデータは決して平文で公開されることはない。

【０１７２】

また、セキュアコンテナとシンク間のセキュアな接続がディフィ・ヘルマン鍵交換方式を利用して確立することにより、公開され普及している方法によってセキュアな接続を確立できる点である。

【０１７３】

また、セキュアコンテナとシンク間のセキュアな接続（ｂ）をＣＰＲＭを利用して確立することができる。ＣＰＲＭを利用することにより、ＳＤカードなど、ＣＰＲＭに対応するあらゆる環境でシステムを利用できる。

【０１７４】

また、ライセンスを保存する別の方法として、ソースとシンクの相互認証を行う段階（ａ）と、シンクに関連付けられた公開鍵をソースに転送する段階（ｂ）と、シンクに関連付けられた公開鍵を用いて暗号化されたライセンスをソースからシンクに転送する段階（ｃ）と、シンクにおいてラインセンスをシンクに関連付けられた秘密鍵によって復号化する段階（ｄ）とにより構成される方法であってもよい。この場合、セキュアコンテナとソースは相互認証を行い、認証が成功すると、デバイスに対応した公開鍵がソースに送付される。ソースでは、受け取った公開鍵を使ってライセンスデータを暗号化し、暗号データをセキュアコンテナに送る。セキュアコンテナでは、受け取ったデータを内部メモリに保存する。

【０１７５】

以上により、ライセンスをセキュアコンテナに保存する時に、ライセンスデータはソースからシンクへセキュアに転送され、シンクのメモリに安全に保存される。ライセンスデータは決して平文で公開されることはない。

【０１７６】

【発明の効果】

以上のように、本発明によれば、専用の再生機器や対応可能なＰＣハードウェアで固有なＩＤを持つものに限定されずに、取得したコンテンツを自由に再生することができ、且つ、デジタルライセンスデータをセキュアに保存・送信するための暗号化アルゴリズムやプロトコルを提供することにより、ライセンスデータの安全管理を保証することが可能となる。

【０１７７】

また、システムに固有な鍵をコンテンツの暗号化に用いることが可能となり、データの盗聴や改ざんを防ぐ安全性をより強化できる。更に、セキュアコンテナやそこに保存されているデジタルライセンスデータが改ざんや乱用を受けた場合、システム制作者や許可された第三者がそれを認識できるようになる。

【０１７８】

また、ある特定のプラットフォームやメディアに制限されることなく、オンラインでもオフラインでもあらゆるメディア配信に用いることができ。デジタルコンテンツやメディアの権利保護に加えて、ソフトウェアや番組配信といったライセンスベースの保護スキームにも適用することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態１におけるセキュアコンテナの構成の一例を示すブロック図

【図２】

本発明の実施の形態２におけるセキュアコンテナの構成の一例を示すブロック図

【図３】

本発明の実施の形態１におけるセキュアコンテナの、トランスコード処理の概要を示す図

【図４】

本発明の実施の形態１におけるセキュアコンテナの、トランスコード処理の流れの一例を示すフローチャート

【図５】

本発明の実施の形態１におけるセキュアコンテナの、トランスコード処理の流れの一例を示すフローチャート

【図６】

本発明の実施の形態１におけるセキュアコンテナの、再暗号化処理の概要を示す図

【図７】

本発明の実施の形態１におけるセキュアコンテナの、再暗号化処理の流れの一例を示すフローチャート

【図８】

本発明の実施の形態１におけるセキュアコンテナの、周期的な再暗号化処理の流れの一例を示すフローチャート

【図９】

本発明の実施の形態１におけるセキュアコンテナの、ライセンスの存在の証明を生成する処理の概要を示す図

【図１０】

本発明の実施の形態１におけるセキュアコンテナの、ライセンスの存在の証明を生成する処理の流れの一例を示すフローチャート

【図１１】

本発明の実施の形態１におけるセキュアコンテナの、ライセンスの存在の証明を生成し、さらにライセンスを変更する処理の概要を示す図

【図１２】

本発明の実施の形態１におけるセキュアコンテナの、ライセンスの存在の証明を生成し、さらにライセンスを変更する処理の流れの一例を示すフローチャート

【図１３】

本発明の実施の形態２におけるセキュアコンテナの、ライセンスを保存する処理の概要を示す図

【図１４】

本発明の実施の形態２におけるセキュアコンテナの、ライセンスを保存する処理の流れの一例を示すフローチャート

【図１５】

本発明の実施の形態１におけるデータ配信システムの概要の一例を示す図

【図１６】

本発明の実施の形態１におけるデータ配信システムの概要の別の一例を示す図

【図１７】

本発明の実施の形態１におけるデータ配信システムのネットワーク環境の概要の一例を示す図

【図１８】

従来のデータ配信システムの概要の一例を示す図

【図１９】

従来のデータ配信システムの概要の別の一例を示す図

【符号の説明】

１００　コンテンツプロバイダー

１０１　暗号化の鍵

１０２　コンテンツ記憶装置

１０３　デバイス依存鍵でコンテンツ暗号化する処理

１０４　ＰＣ

１０５　暗号化コンテンツ記憶装置

１０６　クライアント

１０７　コンテンツを復号化する処理

１０８　コンテンツ記憶装置

１０９　復号化の鍵

２０１　コンテンツプロバイダー

２０２　コンテンツ記憶装置
２０３　鍵を生成する処理
２０４　生成された鍵でコンテンツを暗号化する処理
２０５　ＰＣ
２０６　コンテンツ記憶装置
２０７　鍵記憶装置
２０８　復号化する処理
２０９　暗号化する処理
２１０　セッション鍵
２１１　クライアント
２１２　コンテンツ記憶装置
２１３　セッション鍵
２１４　セッション鍵記憶装置
２１５　復号化する処理
２１６　メディア出力する処理
３００　コンテンツプロバイダー
３０１　コンテンツ記憶装置
３０２　ライセンス（鍵）でコンテンツを暗号化する処理
３０３　ライセンスを生成及びプールする処理
３０４　セッション鍵ＣＰ－Ｃ（コンテンツプロバイダーとクライアントの間
）
３０５　セッション鍵でライセンスを暗号化する処理
３０６　ＰＣ
３０７　コンテンツ記憶装置
３０８　クライアントのＤＲＭデバイス
３０９　セッション鍵でライセンスを復号化する処理
３１０　ライセンス記憶装置
３１１　セッション鍵ＣＰ－Ｃ（コンテンツプロバイダーとクライアントの間
）

３１２　コンテンツをトランスコードする処理

３１３　セッション鍵Ｃ－Ｃ（クライアントのＤＲＭデバイスとクライアントの間）

３１４　セッション鍵Ｃ－Ｃ（クライアントのＤＲＭデバイスとクライアントの間）

３１５　クライアントデータパス

３１６　メディア出力する処理

３１７　コンテンツ記憶装置

３１８　クライアント

４００　外部の記憶装置メディア

５００，６００　セキュアコンテナ

５０１　Ｉ／Ｏポート

５０２　セッションマネージャ

５０３　メモリ管理部

５０４　メモリ

５０５　ユーセッジルール適用部

５０６　ライセンス管理エンジン

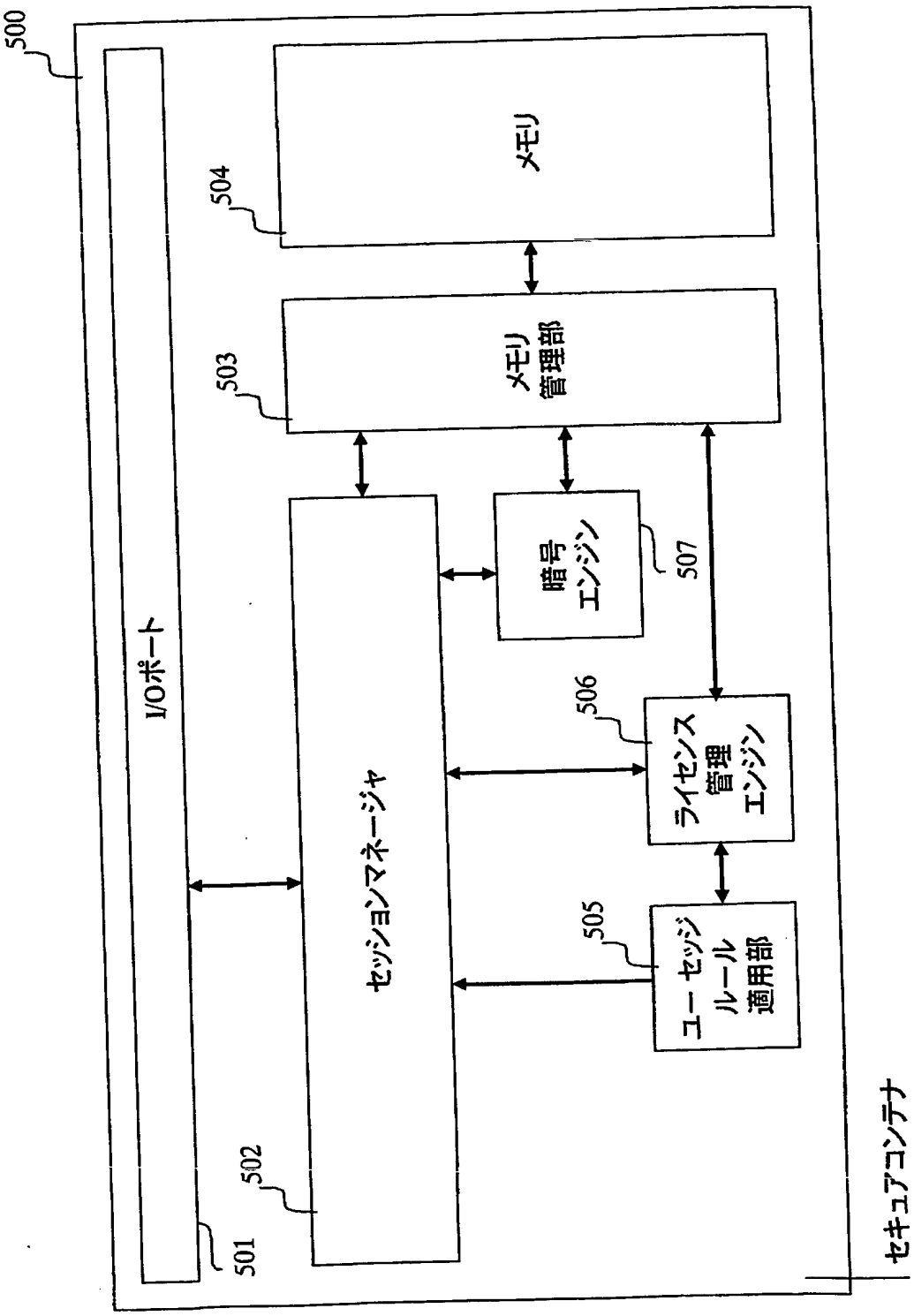
５０７　暗号エンジン

６０１　デバイス依存鍵

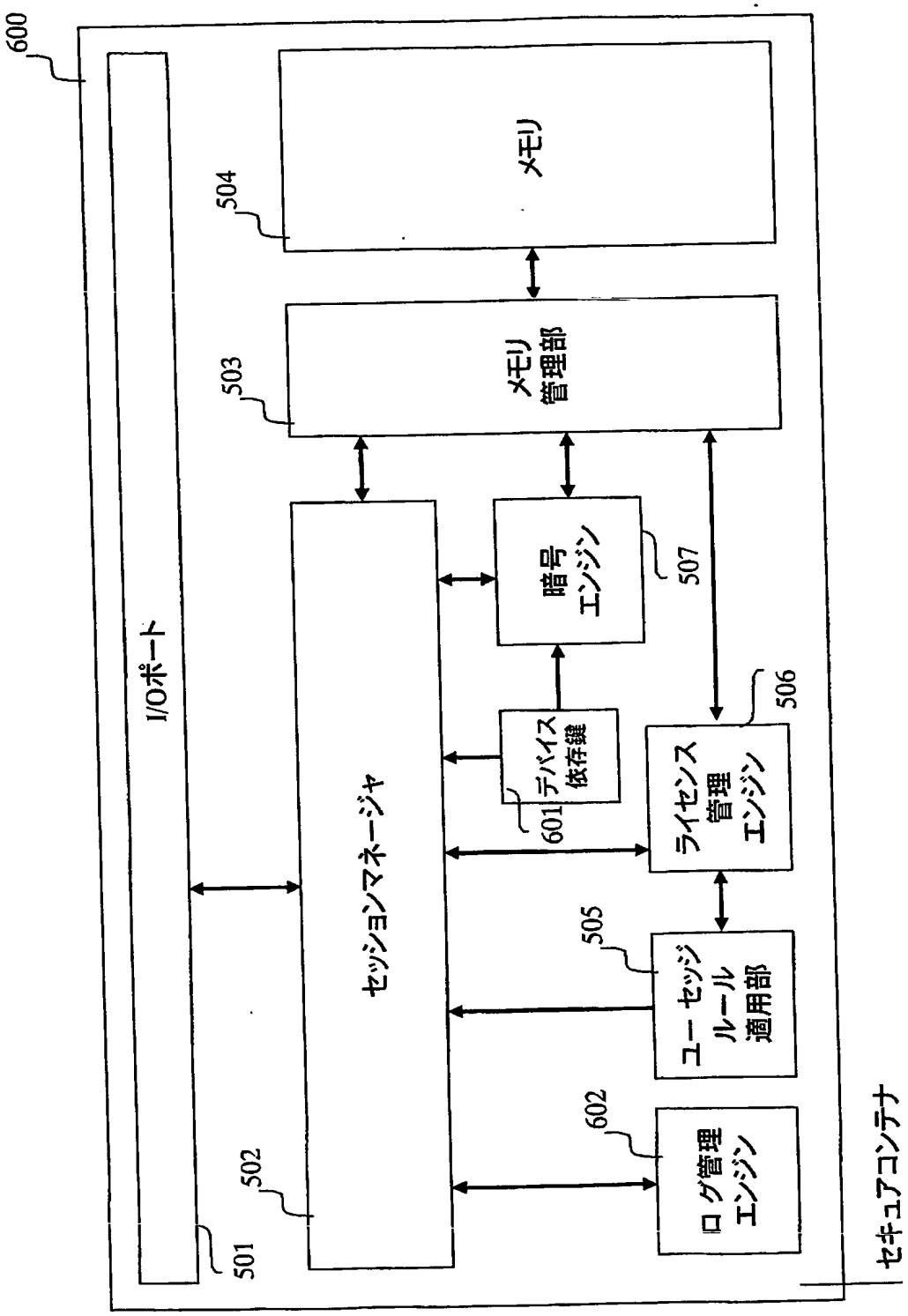
６０２　ログ管理エンジン

【書類名】　図面

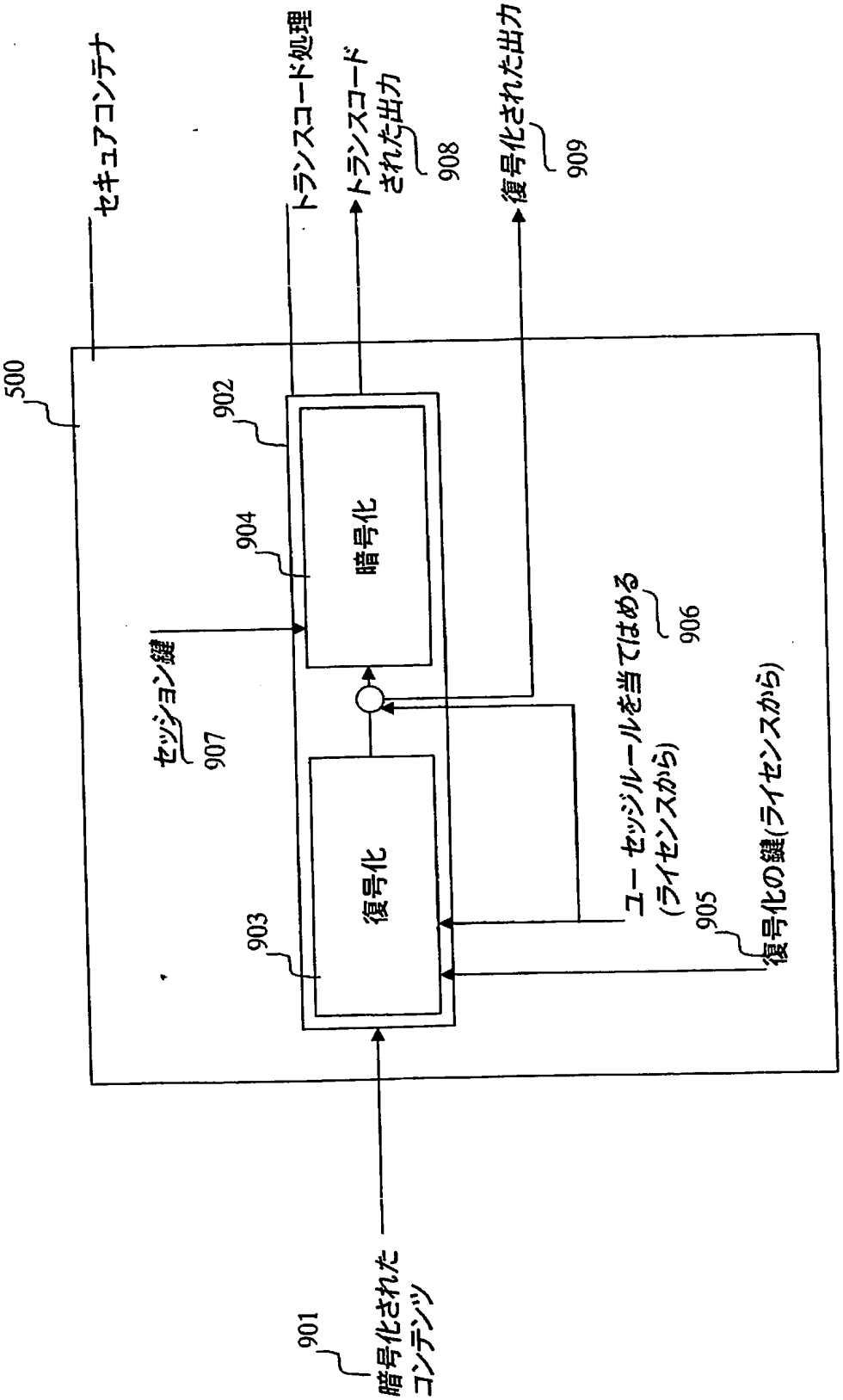
【図１】


500
メモリ
504
メモリ管理部
503
暗号エンジン
507
I/Oポート
セッションマネージャ
506
ライセンス管理エンジン
505
ユーセッションルール適用部
502
501
セキュアコンテナ

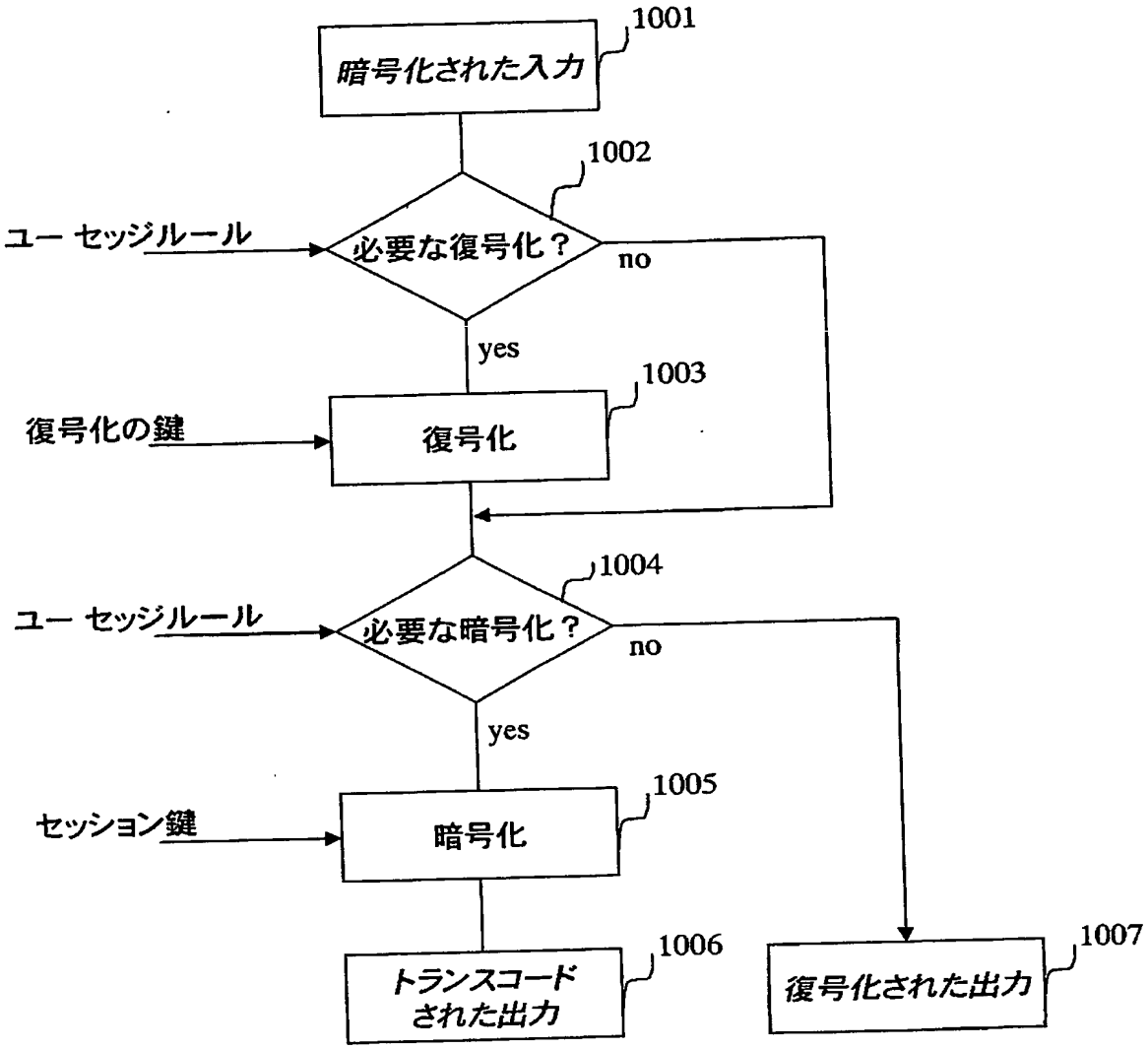
【図２】


600
I/Oポート
501
セッションマネージャ
502
メモリ
504
メモリ管理部
503
暗号エンジン
507
デバイス依存鍵
601
ライセンス管理エンジン
506
ユーセッジルール適用部
505
ログ管理エンジン
602
セキュアコンテナ

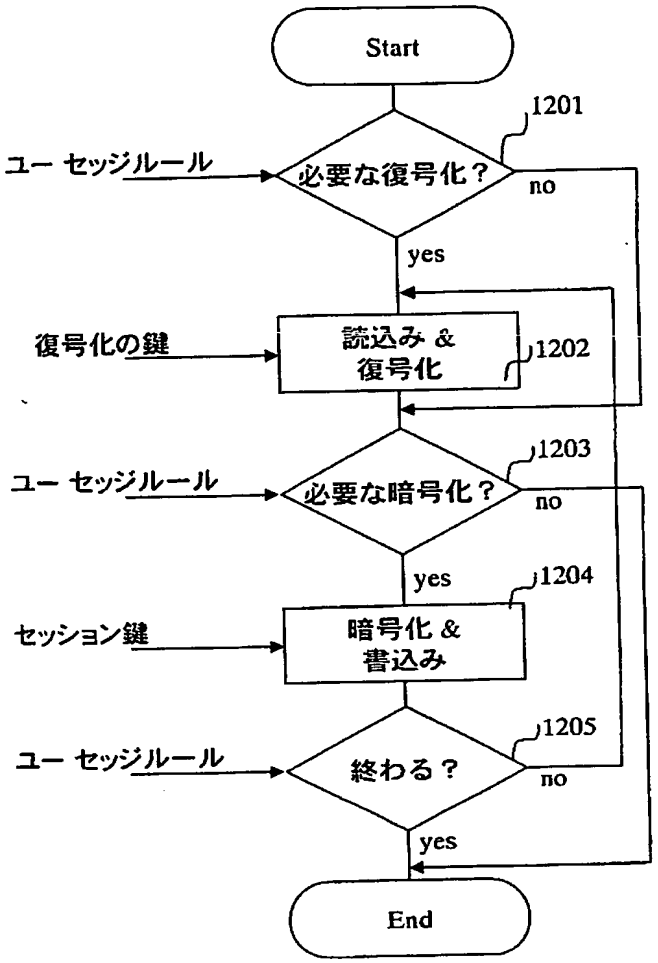
【図３】


セキュアコンテナ
トランスコード処理
トランスコード
された出力
908
復号化された出力
909
500
902
904
暗号化
セッション鍵
907
ユーセッションルールを当てはめる
(ライセンスから)
906
復号化の鍵(ライセンスから)
905
復号化
903
暗号化された
コンテンツ
901

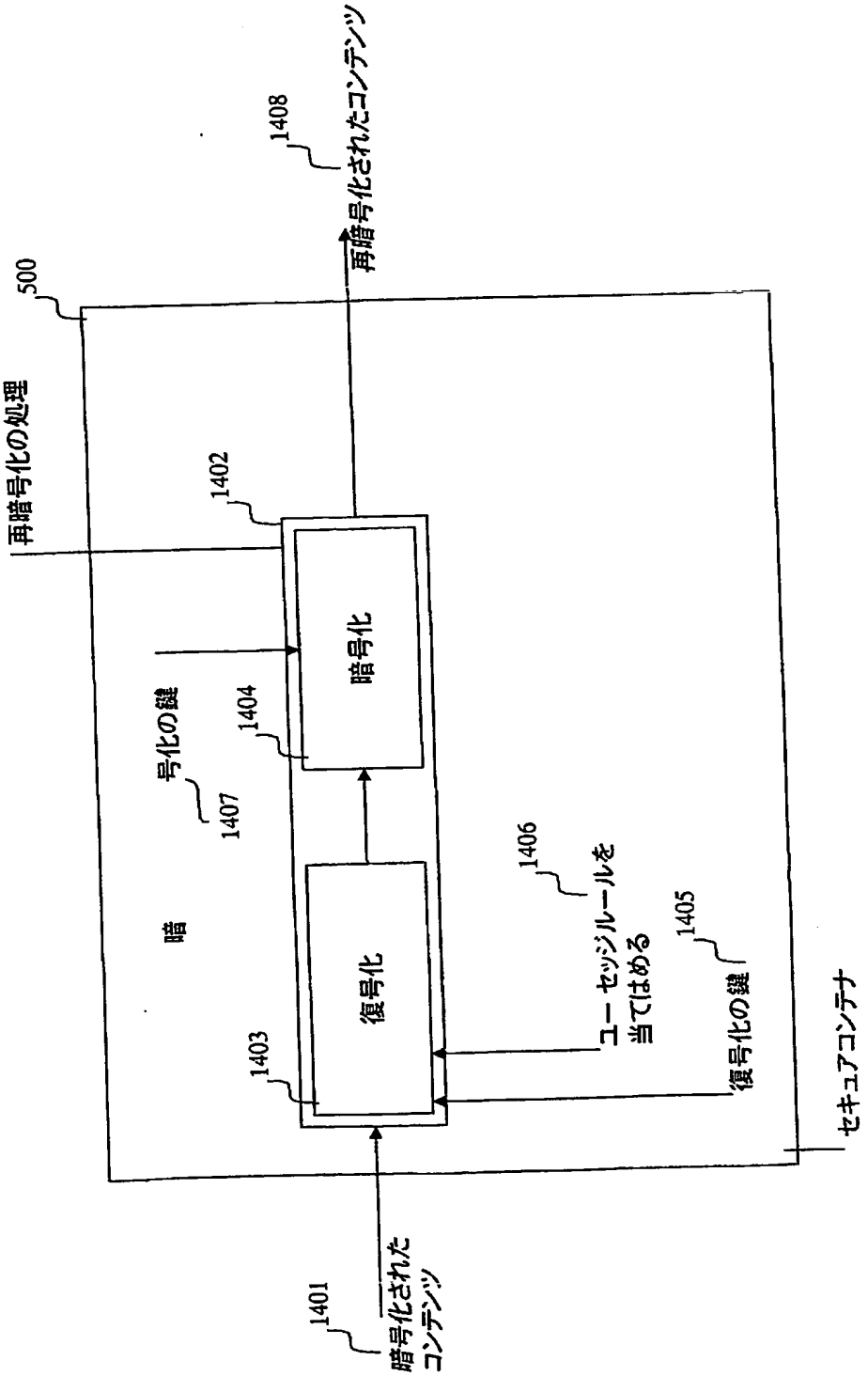
【図４】


1001
暗号化された入力
1002
ユー セッジルール
必要な復号化？
no
yes
1003
復号化の鍵
復号化
1004
ユー セッジルール
必要な暗号化？
no
yes
1005
セッション鍵
暗号化
1006
トランスコード
された出力
1007
復号化された出力

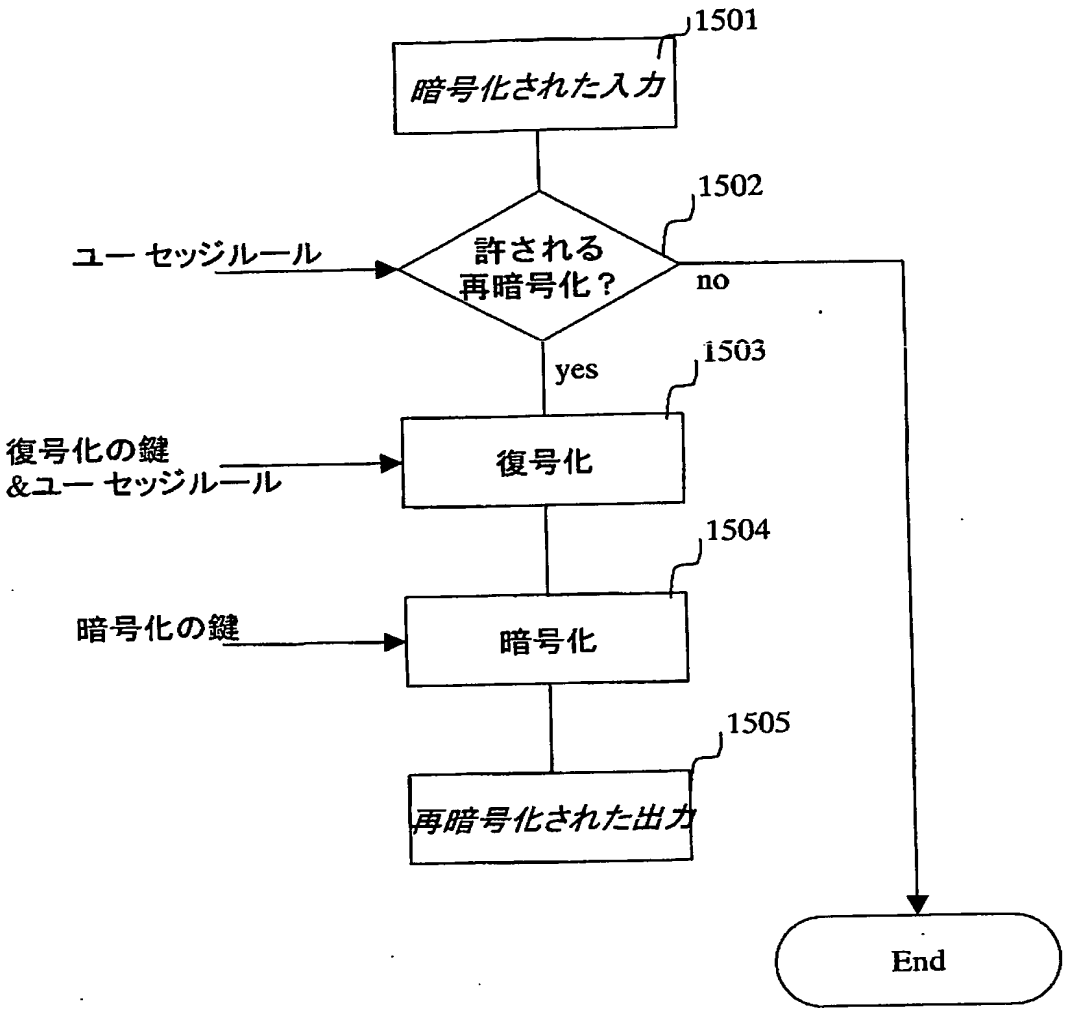
【図５】


Start
1201
ユー セッジルール
必要な復号化？
no
yes
復号化の鍵
読込み &
復号化
1202
1203
ユー セッジルール
必要な暗号化？
no
yes
1204
セッション鍵
暗号化 &
書込み
1205
ユー セッジルール
終わる？
no
yes
End

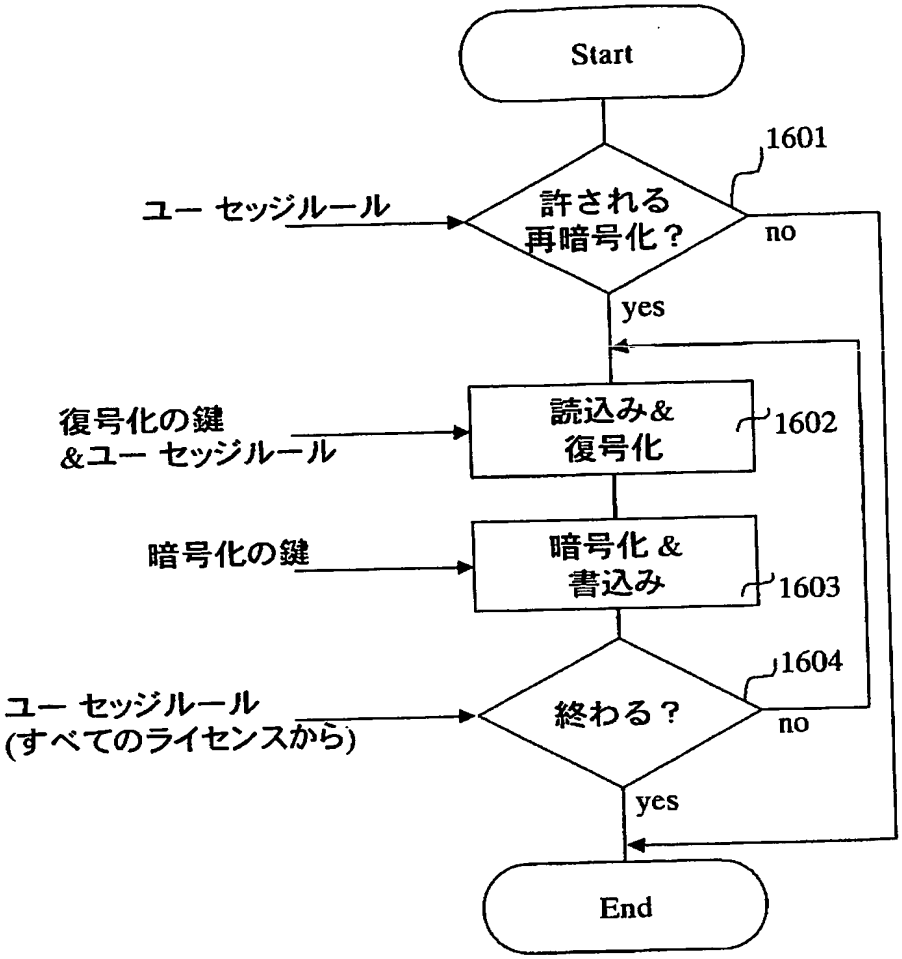
【図６】


1408
再暗号化されたコンテンツ
500
再暗号化の処理
1402
暗号化
暗号化の鍵
1404
1407
暗
復号化
1406
ユーセッジルールを当てはめる
1405
復号化の鍵
1403
セキュアコンテナ
1401
暗号化されたコンテンツ

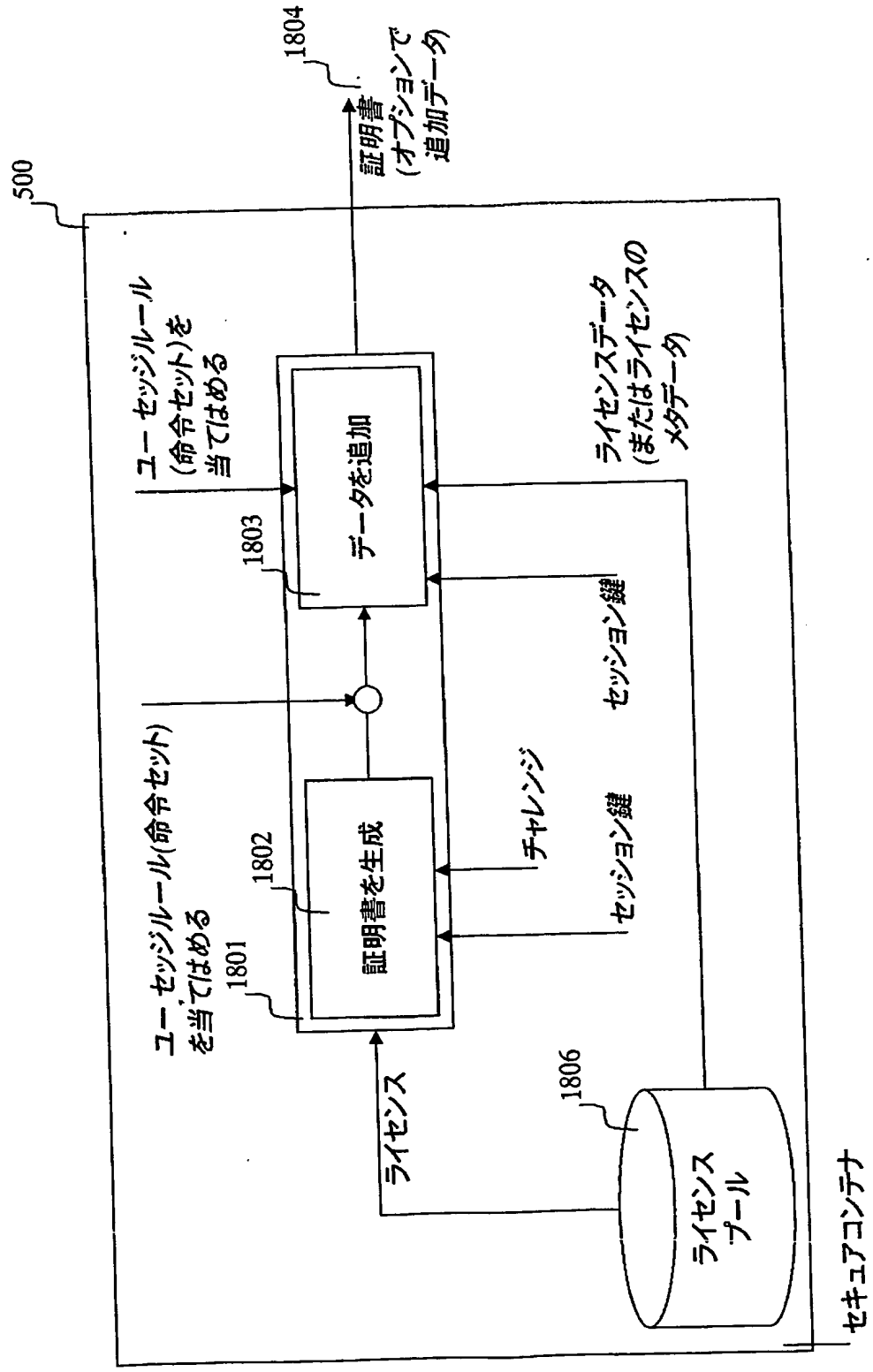
【図７】


1501
暗号化された入力
1502
ユー セッジルール
許される
再暗号化？
no
yes
1503
復号化の鍵
&ユー セッジルール
復号化
1504
暗号化の鍵
暗号化
1505
再暗号化された出力
End

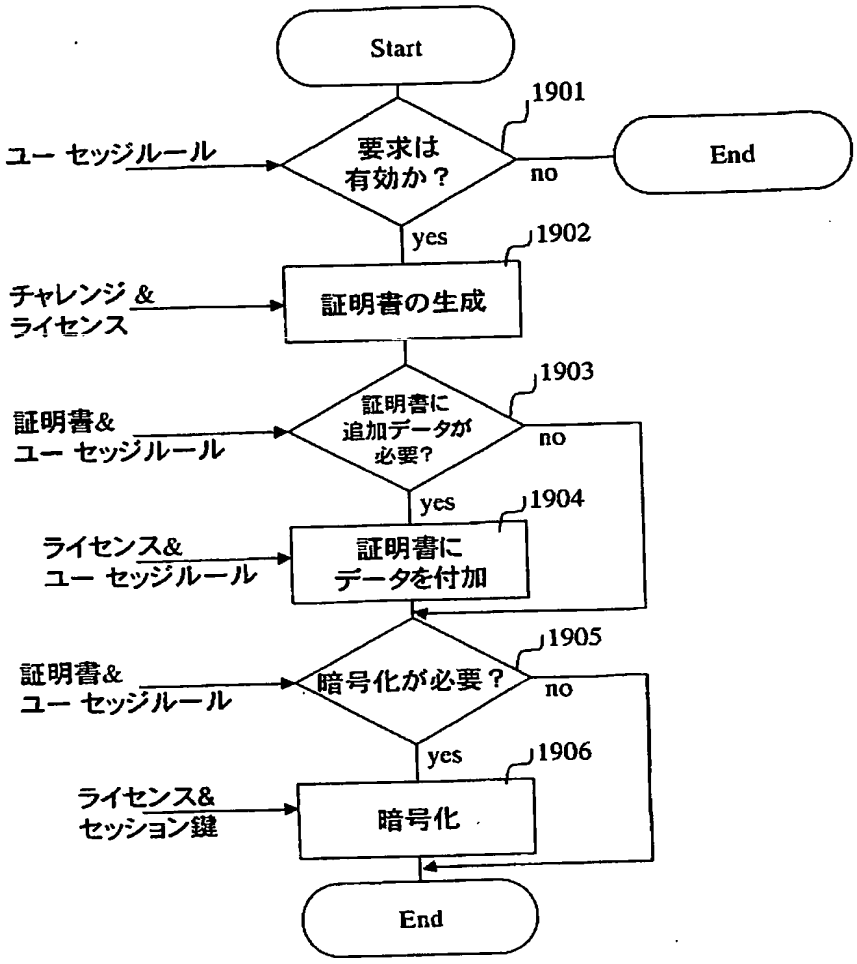
【図８】


Start
1601
ユー セッジルール
許される
再暗号化？
no
yes
復号化の鍵
&ユー セッジルール
読込み&
復号化
1602
暗号化の鍵
暗号化 &
書込み
1603
1604
ユー セッジルール
(すべてのライセンスから)
終わる？
no
yes
End

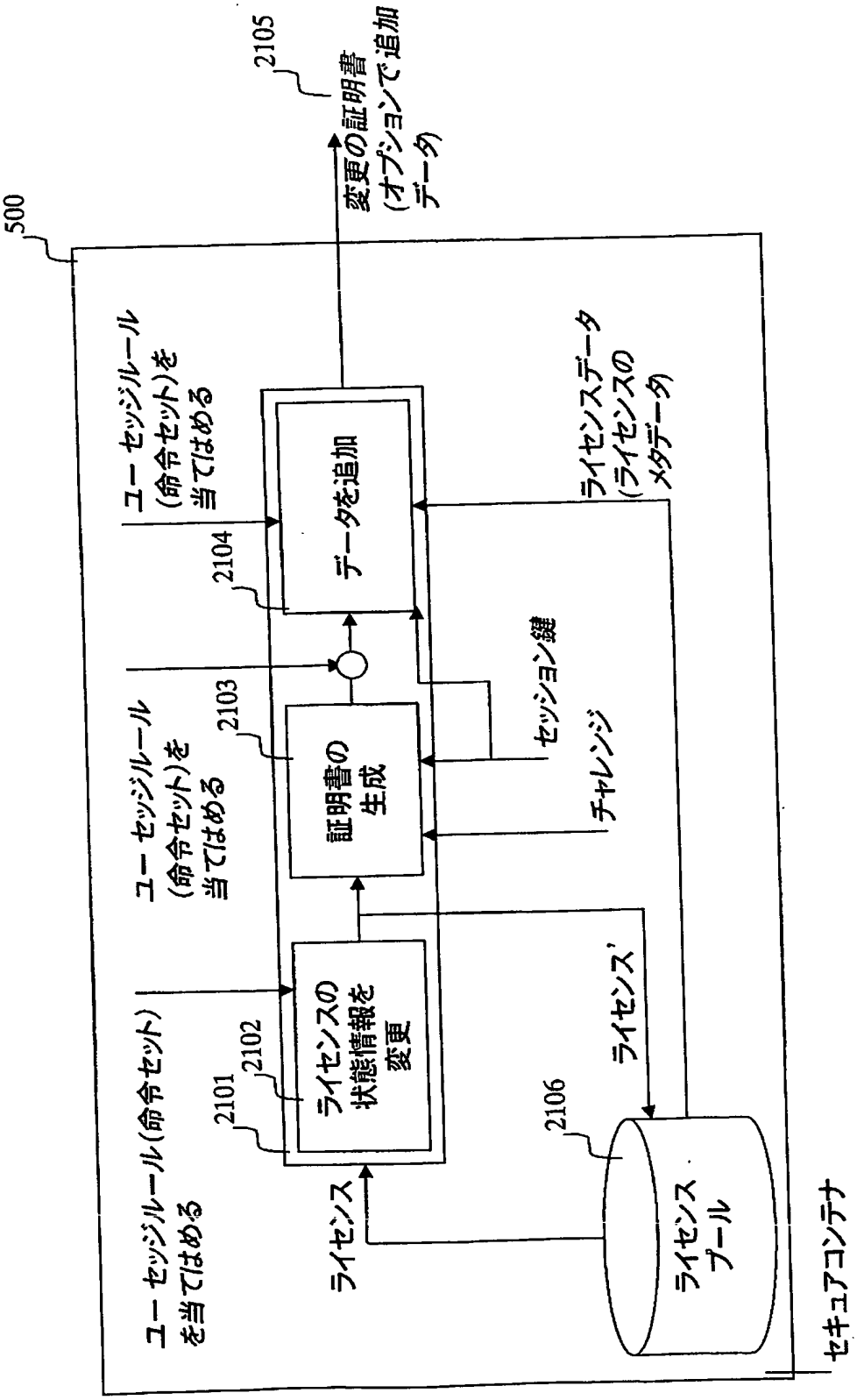
【図９】


500
1804
証明書
(オプションで
追加データ)
ユーセッションルール
(命令セット)を
当てはめる
データを追加
1803
ライセンスデータ
(またはライセンスの
メタデータ)
セッション鍵
ユーセッションルール(命令セット)
を当てはめる
証明書を生成
1802
1801
チャレンジ
セッション鍵
ライセンス
1806
ライセンス
プール
セキュアコンテナ

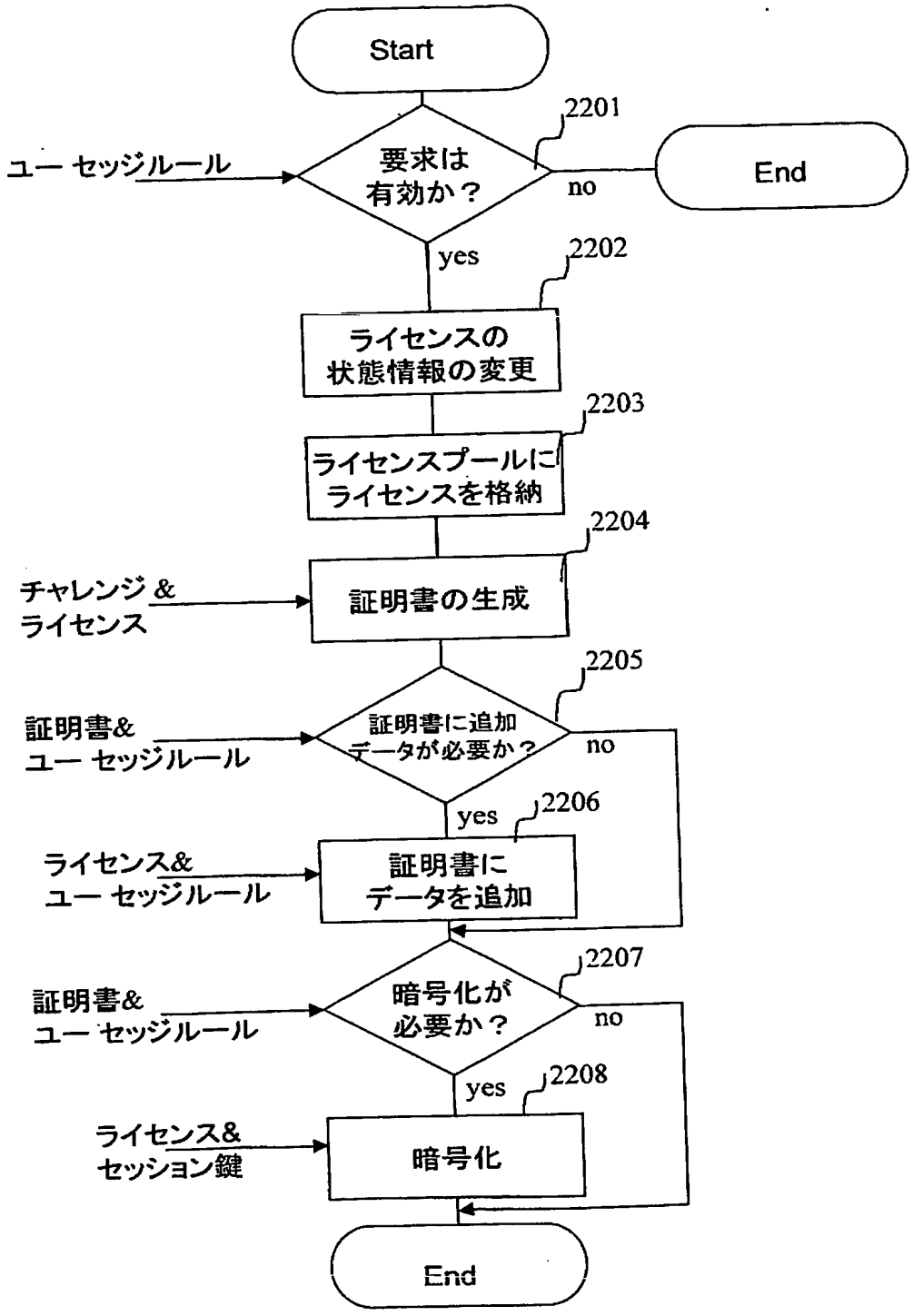
【図１０】


Start
1901
ユー セッジルール
要求は
有効か？
no
End
yes
1902
チャレンジ &
ライセンス
証明書の生成
1903
証明書に
追加データが
必要?
証明書&
ユー セッジルール
no
yes
1904
ライセンス&
ユー セッジルール
証明書に
データを付加
1905
証明書&
ユー セッジルール
暗号化が必要？
no
yes
1906
ライセンス&
セッション鍵
暗号化
End

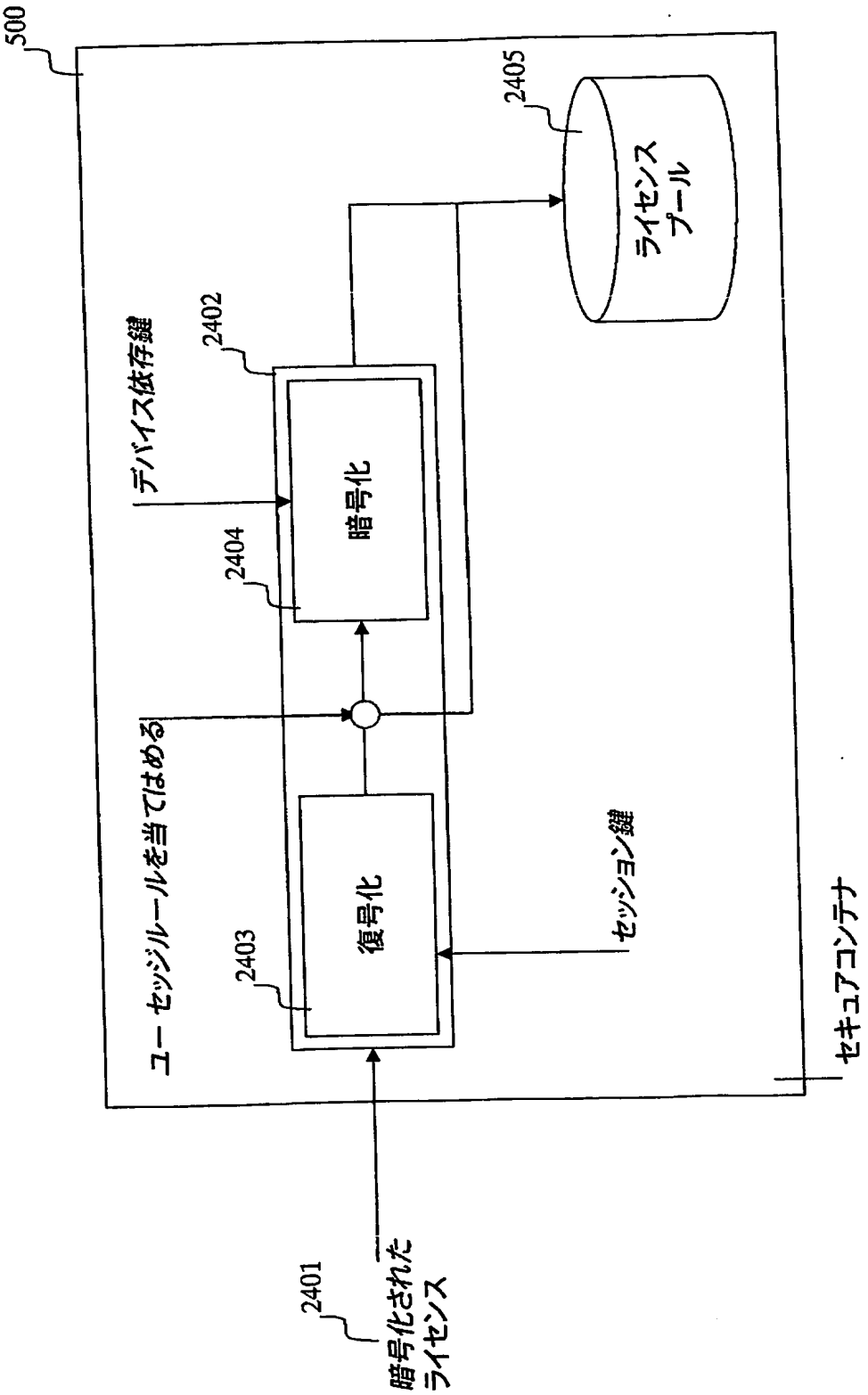
【図１１】


500
2105
変更の証明書
(オプションで追加
データ)
ユーセッジルール
(命令セット)を
当てはめる
2104
データを追加
ライセンスデータ
(ライセンスの
メタデータ)
セッション鍵
2103
証明書の
生成
チャレンジ
ユーセッジルール
(命令セット)を
当てはめる
2102
ライセンスの
状態情報を
変更
ライセンス'
ユーセッジルール(命令セット)
を当てはめる
2101
2106
ライセンス
ライセンス
プール
セキュアコンテナ

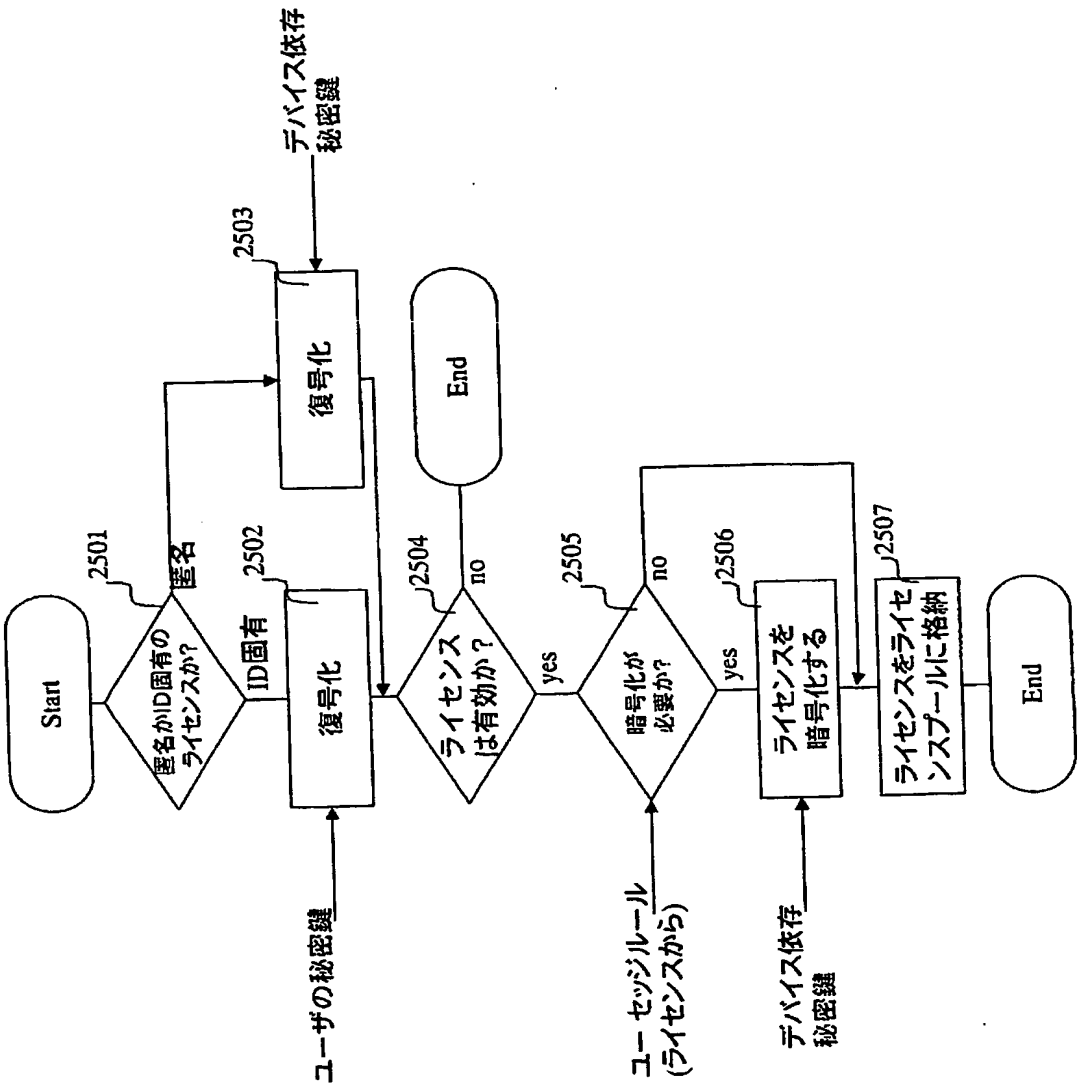
【図１２】


Start
2201
ユー セッジルール
要求は
有効か？
no
End
yes
2202
ライセンスの
状態情報の変更
2203
ライセンスプールに
ライセンスを格納
2204
チャレンジ＆
ライセンス
証明書の生成
2205
証明書&
ユー セッジルール
証明書に追加
データが必要か？
no
yes
2206
ライセンス&
ユー セッジルール
証明書に
データを追加
2207
証明書&
ユー セッジルール
暗号化が
必要か？
no
yes
2208
ライセンス&
セッション鍵
暗号化
End

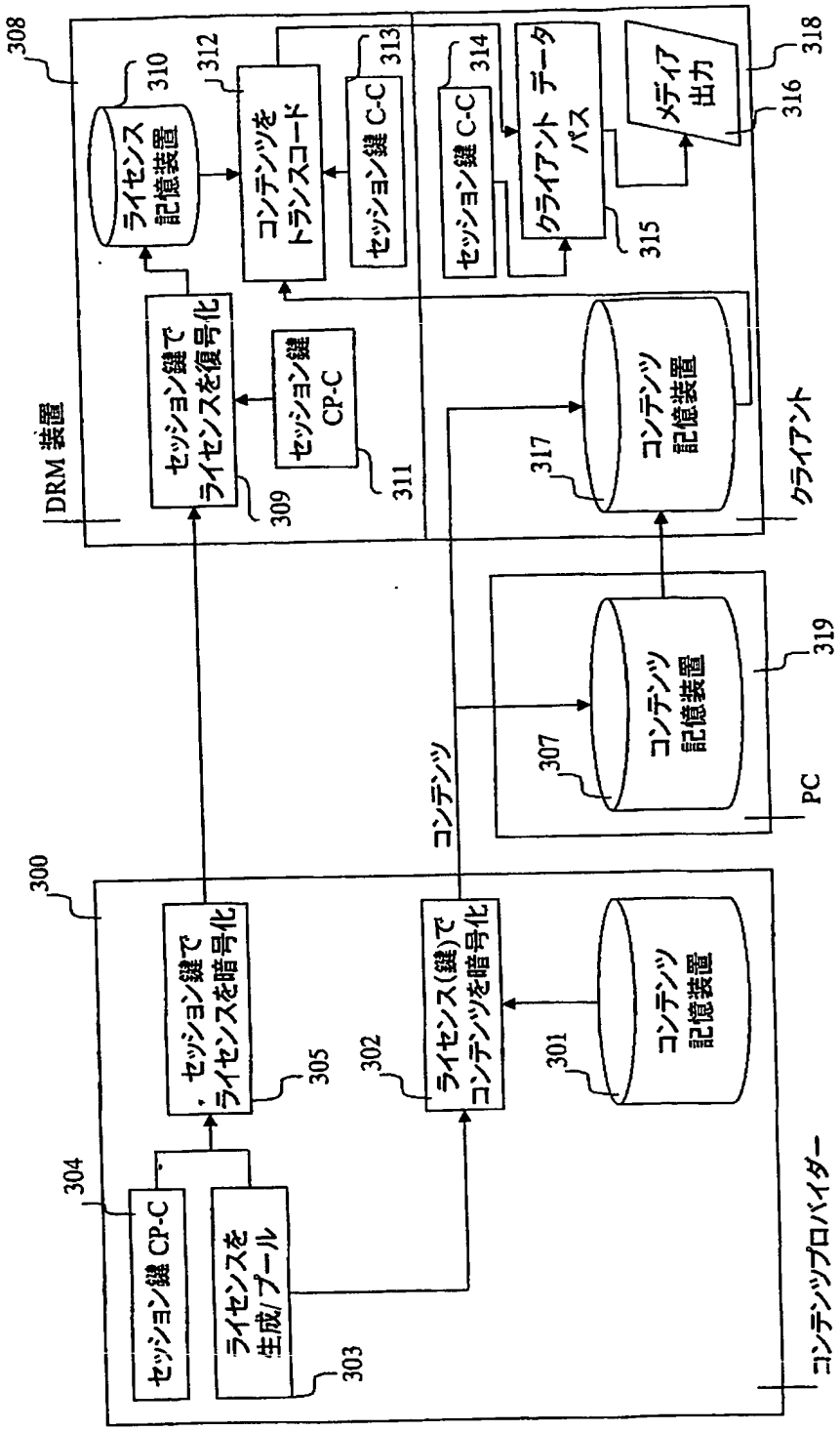
【図１３】


500
2405
ライセンス
プール
2402
デバイス依存鍵
暗号化
2404
ユーセッションルールを当てはめる
復号化
2403
セッション鍵
セキュアコンテナ
2401
暗号化された
ライセンス

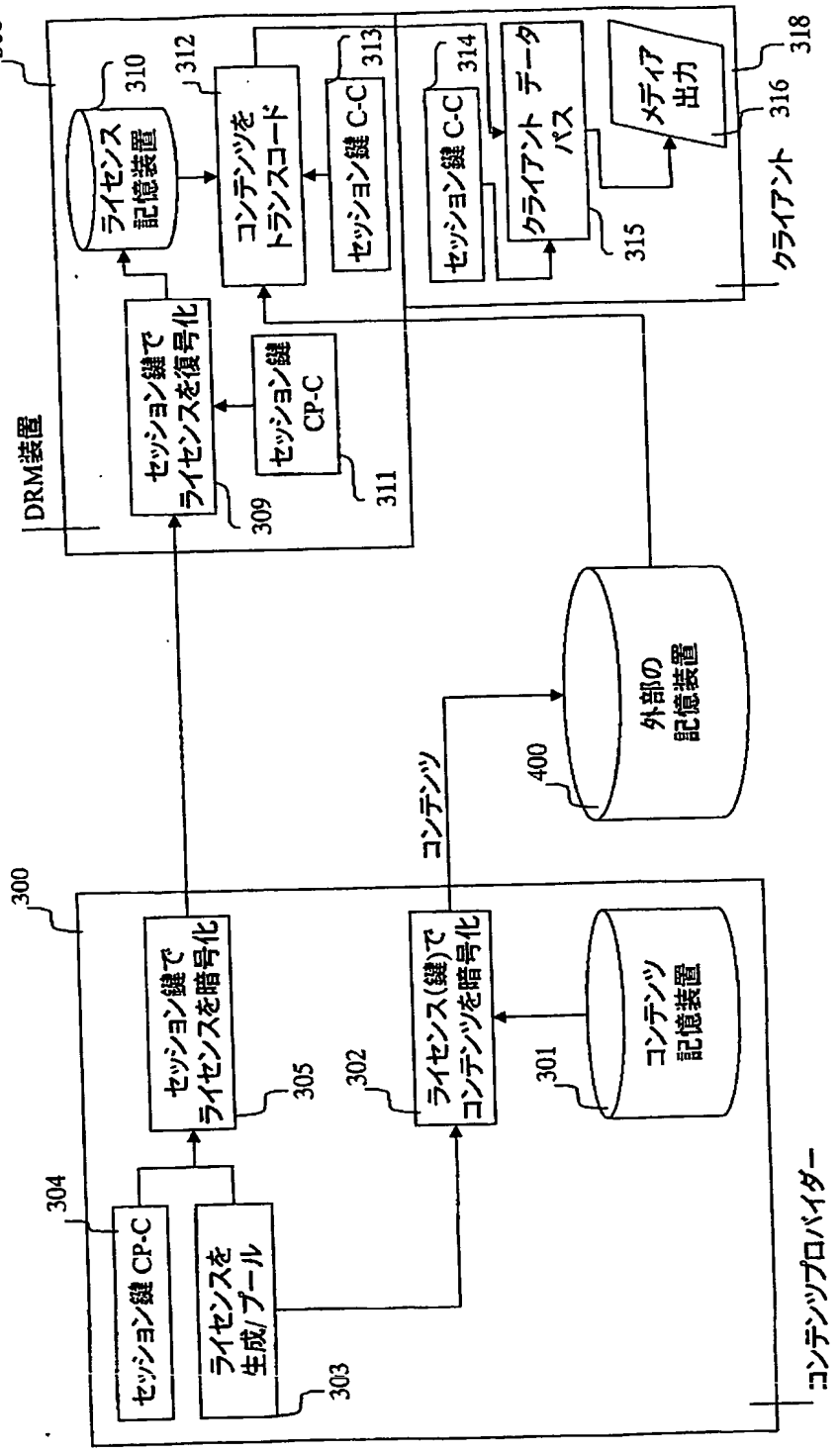
【図１４】


Start
匿名かID固有のライセンスか?
匿名
ID固有
2501
2502
2503
2504
2505
2506
2507
復号化
デバイス依存秘密鍵
ユーザの秘密鍵
ライセンスは有効か?
no
yes
End
暗号化が必要か?
no
yes
ユーザセッションルール(ライセンスから)
ライセンスを暗号化する
デバイス依存秘密鍵
ライセンスをライセンスプールに格納
End

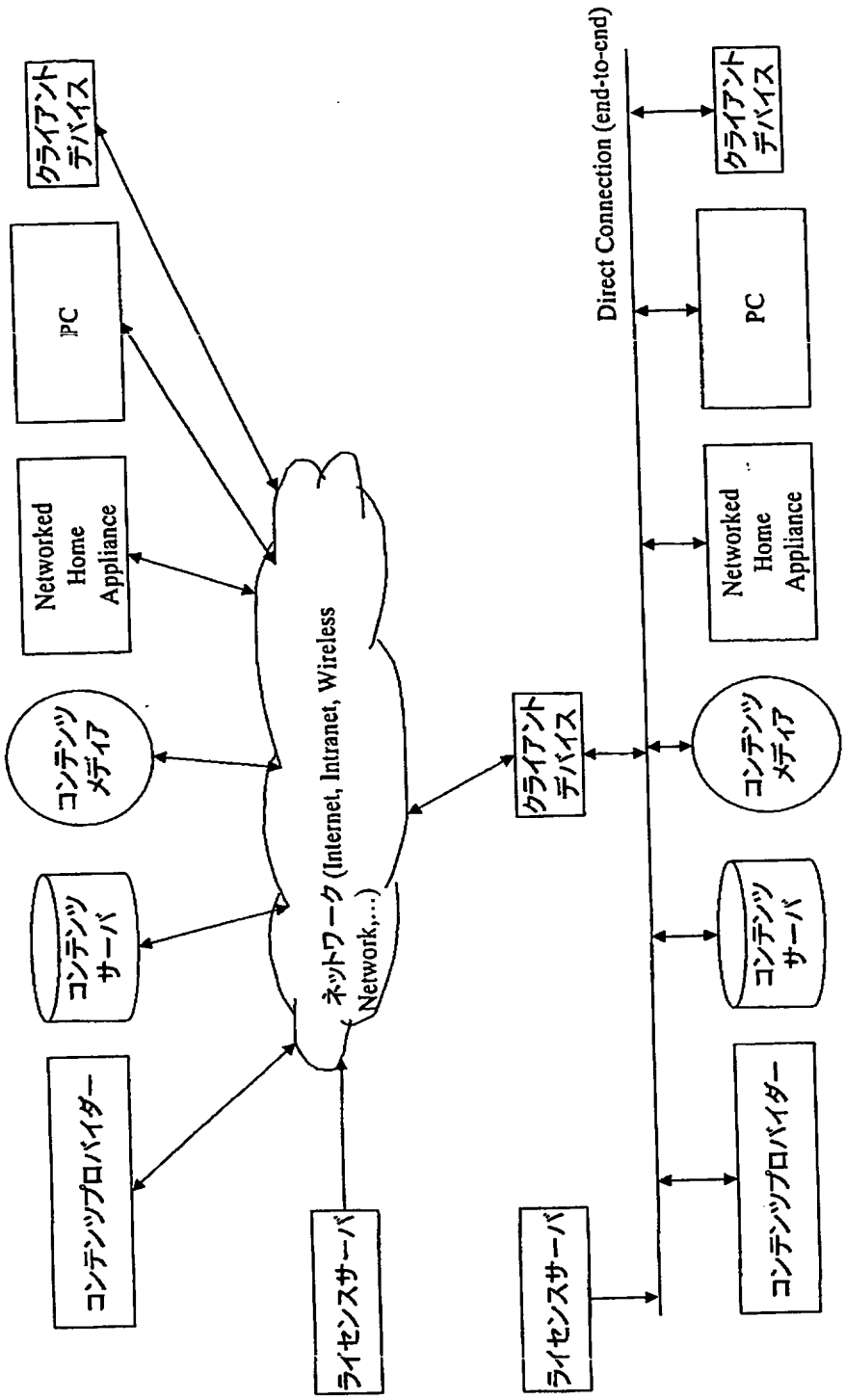
【図１５】


308
310
ライセンス記憶装置
312
コンテンツをトランスコード
313
セッション鍵 C-C
314
セッション鍵 C-C
クライアント データバス
315
メディア出力
316
318
DRM 装置
セッション鍵でライセンスを復号化
309
セッション鍵 CP-C
311
317
コンテンツ記憶装置
クライアント
コンテンツ
307
コンテンツ記憶装置
319
PC
300
セッション鍵でライセンスを暗号化
305
302
ライセンス(鍵)でコンテンツを暗号化
301
コンテンツ記憶装置
304
セッション鍵 CP-C
ライセンスを生成/プール
303
コンテンツプロバイダー

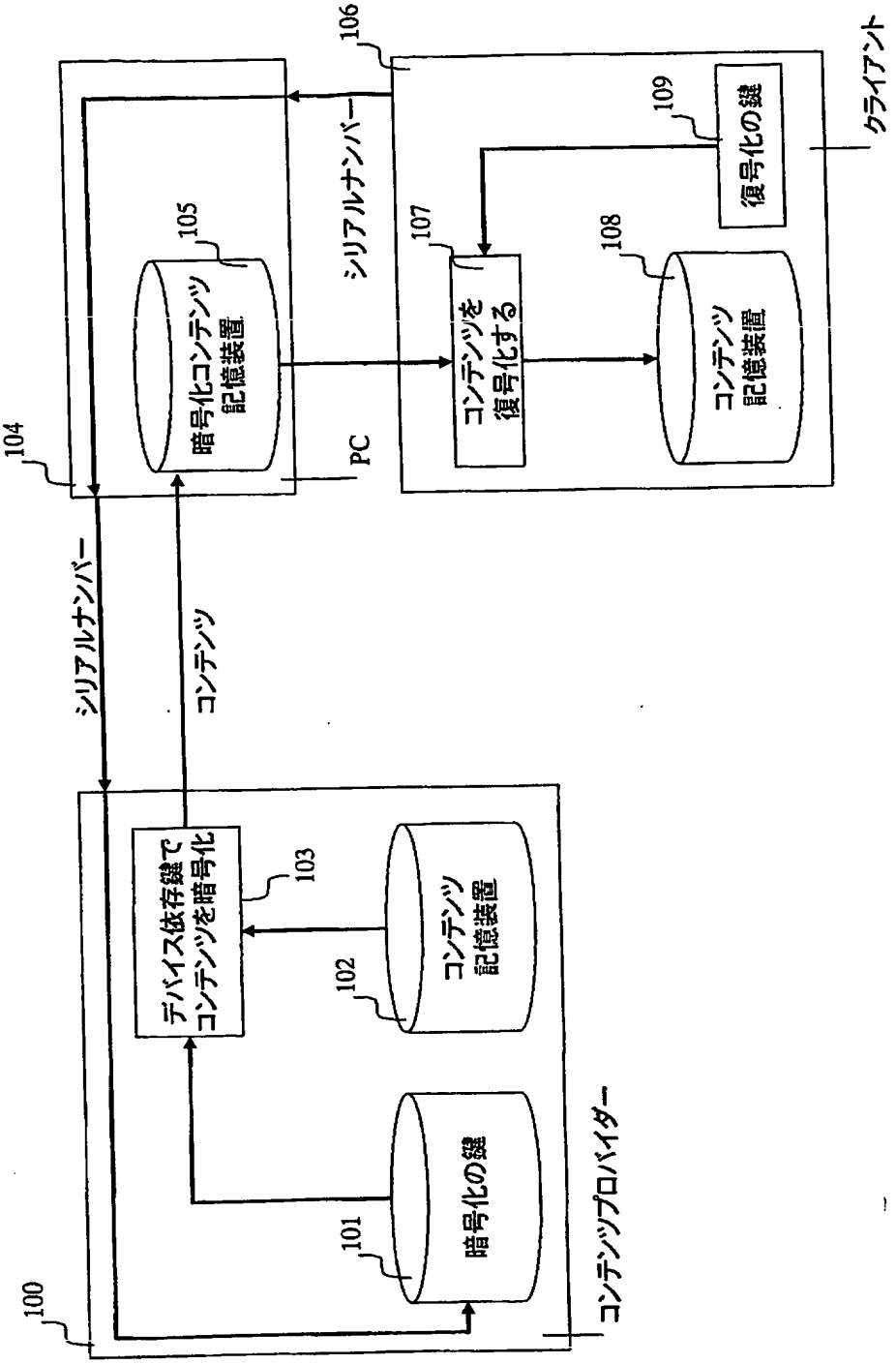
【図１６】


308
310
ライセンス記憶装置
312
コンテンツをトランスコード
313
セッション鍵 C-C
314
セッション鍵 C-C
クライアント データバス
メディア出力
318
316
315
クライアント
DRM装置
セッション鍵でライセンスを復号化
309
セッション鍵 CP-C
311
コンテンツ
400
外部の記憶装置
300
セッション鍵でライセンスを暗号化
305
302
ライセンス(鍵)でコンテンツを暗号化
301
コンテンツ記憶装置
304
セッション鍵 CP-C
ライセンスを生成/プール
303
コンテンツプロバイダー

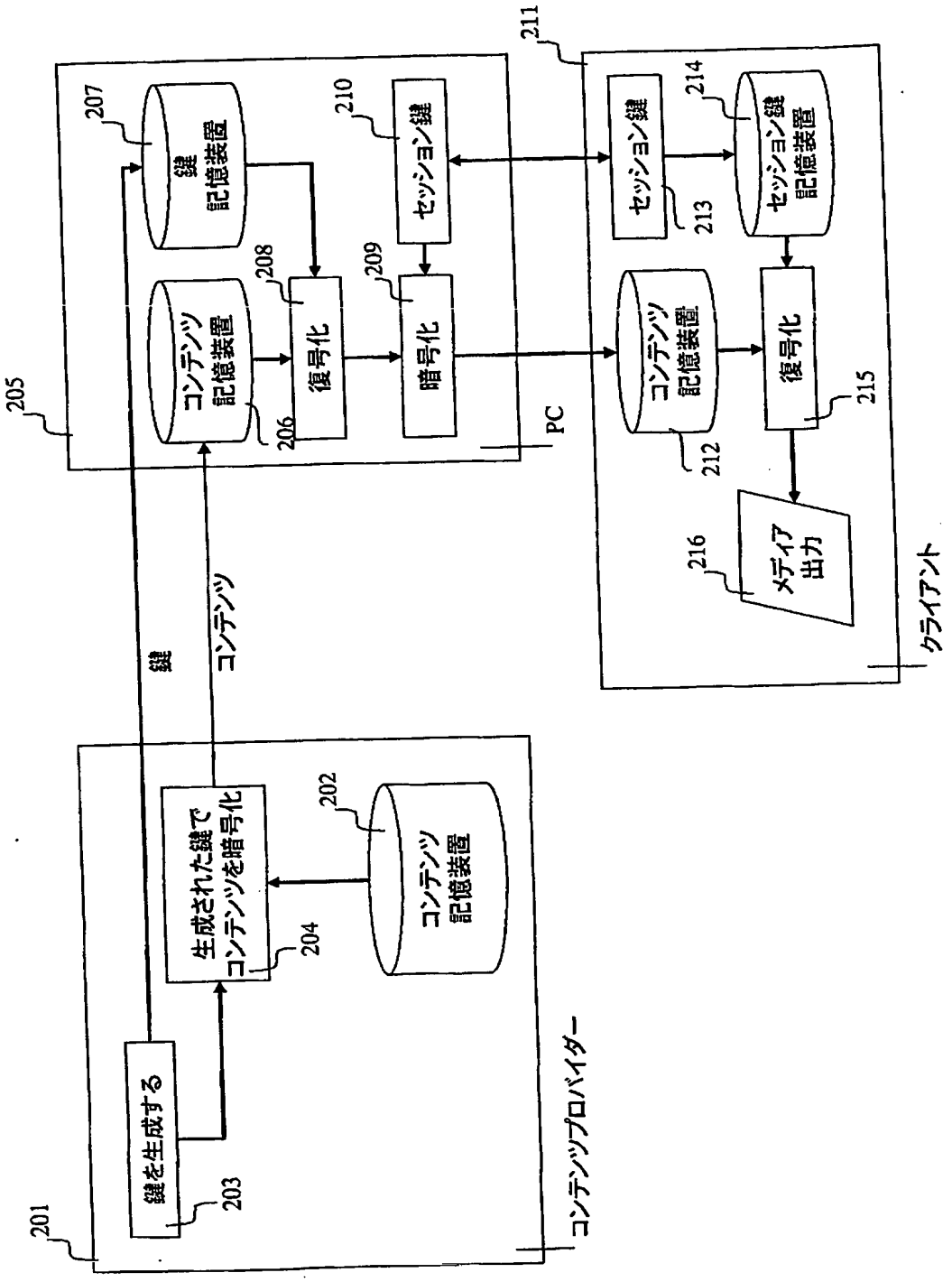
【図１７】


クライアントデバイス
PC
Networked Home Appliance
コンテンツメディア
コンテンツサーバ
コンテンツプロバイダー
ライセンスサーバ
ネットワーク (Internet, Intranet, Wireless Network,...)
クライアントデバイス
Direct Connection (end-to-end)
クライアントデバイス
PC
Networked Home Appliance
コンテンツメディア
コンテンツサーバ
コンテンツプロバイダー
ライセンスサーバ

【図１８】


100
コンテンツプロバイダー
101
暗号化の鍵
102
コンテンツ記憶装置
103
デバイス依存鍵でコンテンツを暗号化
104
PC
105
暗号化コンテンツ記憶装置
106
クライアント
107
コンテンツを復号化する
108
コンテンツ記憶装置
109
復号化の鍵
シリアルナンバー
コンテンツ
シリアルナンバー

【図１９】


201
203
鍵を生成する
204
生成された鍵で
コンテンツを暗号化
202
コンテンツ
記憶装置
コンテンツプロバイダー
鍵
コンテンツ
205
207
鍵
記憶装置
コンテンツ
記憶装置
206
208
復号化
210
セッション鍵
209
暗号化
PC
211
セッション鍵
213
214
セッション鍵
記憶装置
コンテンツ
記憶装置
212
復号化
215
216
メディア
出力
クライアント

【書類名】　要約書

【要約】

【課題】　デジタルライセンスやデジタルデータを保護することにより、デジタルデータの乱用や不正利用を防止し、且つユーザに再生機器に対する選択の自由を与えることを目的とする。

【解決手段】　Ｉ／Ｏポートと、セッションマネージャと、ライセンス管理エンジンと、ユーセッジルール適用部と、暗号エンジンと、メモリ管理部と、メモリとを備え、ライセンス管理エンジンは、セッションマネージャで確立したセッションによってライセンスを取得、保存、管理し、ユーセッジルール適用部は、ライセンス管理エンジンが管理するライセンスの使用に関し、ユーセッジルールを適用することにより、デジタルライセンスデータをセキュアに保存・送信するための暗号化アルゴリズムやプロトコルを提供する。

【選択図】　図１

特願２００３－０８０２６６

出願人履歴情報

識別番号　[０００００５８２１]

１．変更年月日　１９９０年　８月２８日
[変更理由]　新規登録
住所　大阪府門真市大字門真１００６番地
氏名　松下電器産業株式会社